A SYSTEM AND METHOD FOR DYNAMIC FOB SYNCHRONIZATION AND PERSONALIZATION

Cross Reference to Related Applications

This invention may be a continuation in part of U.S. Serial No. 10/340,352, filed on January 10, 2003, and entitled "SYSTEM AND METHOD FOR INCENTING PAYMENT USING RADIO FREQUENCY IDENTIFICATION IN CONTACT AND CONTACTLESS TRANSACTIONS." The '352 application itself claims priority to U.S. Patent Application No. 10/192,488, entitled "SYSTEM AND METHOD FOR PAYMENT USING RADIO FREQUENCY IDENTIFICATION IN CONTACT AND CONTACTLESS TRANSACTIONS," filed on July 9, 2002 (which itself claims priority to U.S. Provisional No. 60/304,216, filed on July 10, 2001); U.S. Patent Application No. 10/318,432, entitled "SYSTEM AND METHOD FOR SELECTING LOAD OPTIONS FOR USE IN RADIO FREQUENCY IDENTIFICATION IN CONTACT AND CONTACTLESS TRANSACTIONS," filed December 13, 2002; U.S. Patent Application No. 10/318,480, entitled "SYSTEM AND METHOD FOR PAYMENT USING RADIO FREQUENCY IDENTIFICATION IN CONTACT AND CONTACTLESS TRANSACTIONS," filed December 13, 2002; and, U.S. Provisional Patent Application No. 60/396,577, filed July 16, 2002. All of the above applications are hereby incorporated by reference.

Technical Field

[0001] The present invention relates generally to the use of Radio Frequency Identification (RFID) in contactless environments for commercial transactions and, more particularly, to a method and system to facilitate dynamic synchronization and personalization of fob information in the context of a distributed transaction system.

Background Art and Technical Problems

[0002] Like barcode and voice data entry, RFID is a contactless information acquisition technology. RFID systems are wireless, and are usually extremely effective in hostile environments where conventional acquisition methods fail. RFID has established itself in a wide range of markets, such as, for example, the high-speed reading of railway containers, tracking moving objects such as livestock or automobiles, and retail inventory applications. As such, RFID technology has become a primary focus in automated data collection, identification and analysis systems worldwide.

[0003] Of late, companies are increasingly embodying RFID data acquisition technology in a fob or tag for use in completing financial transactions. A typical fob may include a transponder and is ordinarily a self-contained device which may be contained on any portable form factor. In some instances, a battery may be included with the fob to power the transponder, in which case the internal circuitry of the fob (including the transponder) may draw its operating power from the battery power source. Alternatively, the fob may exist independent of an internal power source. In this instance the internal circuitry of the fob (including the transponder) may gain its operating power directly from a RF interrogation signal. U.S. Patent No. 5,053,774, issued to Schuermann, describes a typical transponder RF interrogation system which may be found in the prior art. The Schuermann patent describes in general the powering technology surrounding conventional transponder structures. U.S. Patent No. 4,739,328, discusses a method by which a conventional transponder may respond to a RF interrogation signal. Other typical modulation techniques which may be used include, for example, ISO/IEC 14443 and the like.

[0004] In the conventional fob powering technologies used, the fob is typically activated upon presenting the fob in an interrogation signal. In this regard, the fob may be activated irrespective of whether the user desires such activation. Inadvertent presentation of the fob may result in initiation and completion of an unwanted transaction. Thus, a fob system is

needed which allows the fob user to control activation of the fob to limit transactions being undesirably completed.

[0005] One of the more visible uses of the RFID technology is found in the introduction of Exxon/Mobil's Speedpass® and Shell's EasyPay® products. These products use transponders placed in a fob or tag which enables automatic identification of the user when the fob is presented at a Point of Sale (POS) device. Fob identification data is typically passed to a third party server database, where the identification data is referenced to a customer (*e.g.*, user) credit or debit account. In an exemplary processing method, the server seeks authorization for the transaction by passing the transaction and account data to an authorizing entity. Once the server receives authorization, clearance is sent to the POS device for completion of the transaction. In this way, the conventional transaction processing method involves an indirect path which causes undue overhead due to the use of the third-party server.

[0006] It is desirable to maintain, for each fob held by a consumer, a substantially accurate history of transaction information and applications associated with the fob. Presently known systems are typically inadequate in this regard in that they do not provide efficient and reliable methods for ensuring synchronization between information stored on the fob and corresponding information stored on one or more external databases. As a result, present systems fail to ensure that lost or stolen fobs may be reissued or replaced with up-to-date information.

[0007] Moreover, present systems are inadequate in that the systems often do not allow an enterprise, such as a fob corporate partner (for example, Hertz, Hilton and the like) to dynamically add to or otherwise modify the fob application structure itself. That is, in the context of multi-function fobs, it is often infeasible to alter or augment the fob's file structure without engaging in the time-consuming and costly process of re-issuing the fob.

[0008] Furthermore, known methods of issuing and re-issuing fobs in a multi-application, multi-enterprise environment are typically inadequate. More particularly, a fob often

contains a number of different applications associated with a wide range of enterprise organizations. For security purposes, the writing, updating, and reading of these files is advantageously restricted to particular parties in accordance with a set of access condition rules. These access conditions may be suitably implemented using cryptographic keys which are known only to the appropriate parties, such as the enterprise. Thus, a fob issuing party such as American Express will typically not have access to the keys to perform its function. Some of the known systems have attempted to solve this problem by accumulating key data in a central repository used in the issuance process. This method is often unsatisfactory in a number of respects. Most notably, a security breach in the central repository of key information may have disastrous consequences.

[0009] Techniques are therefore needed to overcome these and other limitations of the prior art. More specifically, systems are needed to provide secure and efficient personalization and dynamic synchronization of multi-function fobs.

Summary of the Invention

[0010] The present invention overcomes the limitations of the prior art by providing a system and method for personalizing and synchronizing fob data in the context of a distributed transaction system.

[0011] In accordance with one aspect of the present invention, a dynamic fob synchronization system may comprise POS devices configured to initiate a transaction in conjunction with a fob, an enterprise data collection unit, and a fob object database update system. An exemplary dynamic synchronization system (DSS) may comprise various fob POS devices a secure support client server, a fob object database update system (FODUS), one or more enterprise data synchronization interfaces (EDSIs), an update logic system, one or more enterprise data collection units (EDCUs), and one or more point of sale (POS) devices configured to interoperably accept and interface with fobs. In an exemplary

embodiment, DSS may comprise a personalization system and an account maintenance system configured to communicate with FODUS.

[0012] In accordance with a further aspect of the present invention, personalization of multi-function fobs is accomplished using a security server configured to generate and/or retrieve cryptographic key information from multiple enterprise key systems during the final phase of the fob issuance process.

Brief Description of the Drawings

[0013] The accompanying drawings, wherein like numerals depict like elements, illustrate exemplary embodiments of the present invention, and together with the description, serve to explain the principles of the invention. In the drawings:

[0014] FIG. 1 illustrates an exemplary RFID-based system in accordance with the present invention, wherein exemplary components used for fob transaction completion are depicted;

[0015] FIG. 2 is a schematic illustration of an exemplary fob in accordance with the present invention;

[0016] FIG. 3 is a schematic illustration of an exemplary RFID reader in accordance with the present invention;

[0017] FIG. 4 is an exemplary flow diagram of an exemplary authentication process in accordance with the present invention;

[0018] FIG. 5 is an exemplary flow diagram of an exemplary decision process for a protocol/sequence controller in accordance with the present invention;

[0019] FIG. 6 is an example of a conventional magnetic stripe track 2 layout for MasterCard;

[0020] FIG. 7 is an exemplary transaction data structure suitable for use in a travel context;

[0021] FIG. 8 is a flow diagram of an exemplary payment/transaction process in accordance with the present invention;

[0022] FIG. 9 is another schematic illustration of an exemplary fob in accordance with the present invention;

[0023] FIG. 10 is a schematic overview of an exemplary dynamic synchronization system in accordance with various aspects of the present invention;

[0024] FIG. 11 is a schematic overview of an exemplary secure support client server;

[0025] FIG. 12 is a schematic overview of an exemplary enterprise data synchronization interface;

[0026] FIG. 13 is a schematic overview of an exemplary update logic system;

[0027] FIG. 14 is a schematic overview of an exemplary enterprise data collection unit;

[0028] FIG. 15 is a schematic overview of an exemplary fob object database update system (FODUS);

[0029] FIG. 16 is a flowchart depicting an exemplary method for synchronizing pending transaction information;

[0030] FIG. 17 is a flowchart depicting an exemplary method for synchronizing update transaction information;

[0031] FIG. 18 is a schematic overview of an exemplary personalization system; and

[0032] FIG. 19 is a flowchart depicting an exemplary method of fob personalization.

Detailed Description of Preferred Exemplary Embodiments

[0033] 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 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), JavaFob 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.

[0034] 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 may be noted that the network may be implemented as other types of networks, such as an interactive television network (ITN).

[0035] Where required, the system user may interact with the system via any input device such as, a keypad, keyboard, mouse, kiosk, personal digital assistant, handheld computer (*e.g.*, Palm Pilot®, Blueberry®), cellular phone and/or the like. Similarly, the invention could be used in conjunction with any type of personal computer, network computer, work station, minicomputer, mainframe, or the like running any operating system such as any version of Windows, Windows NT, Windows 2000, Windows 98, Windows 95, MacOS, OS/2, BeOS, Linux, UNIX, Solaris or the like. Moreover, although the invention may frequently be described as being implemented with TCP/IP communications protocol, it should be understood that the invention could also be implemented using SNA, IPX, Appletalk, IPte, NetBIOS, OSI or any number of communications protocols. Moreover, the system contemplates, the use, sale, or distribution of any goods, services or information over any network having similar functionality described herein.

[0036] FIG. 1 illustrates an exemplary RFID transaction system 100 in accordance with the present invention, wherein exemplary components for use in completing a fob transaction using travel-related information are depicted. In general, the operation of system 100 may begin when fob 102 may be presented for payment, and may be interrogated by RFID reader

104 or, alternatively, interface 134. Fob 102 and RFID reader 104 may then engage in mutual authentication after which the fob 102 may provide the transponder identification, account identifier and/or travel-related information to the RFID reader 104 which may further provide the information to the merchant system 130 POS device 110.

[0037] System 100 may include a fob 102 having a transponder 114 and a RFID reader 104 in RF communication with fob 102. Although the present invention may be described with respect to a fob 102, the invention may be not to be so limited. Indeed, system 100 may include any device having a transponder which may be configured to communicate with a RFID reader 104 via RF communication. Typical devices may include, for example, a key ring, tag, fob, cell phone, wristwatch or any such form capable of being presented for interrogation.

[0038] RFID reader 104 may be configured to communicate using a RFID internal antenna 106. Alternatively, RFID reader 104 may include an external antenna 108 for communications with fob 102, where the external antenna may be made remote to RFID reader 104 using a suitable cable and/or data link 120. RFID reader 104 may be further in communication with a merchant system 130 via a data link 122. System 100 may include a transaction completion system including a point of interaction device such as, for example, a merchant point-of-sale (POS) device 110 or a computer interface (*e.g.*, user interface) 134. In one exemplary embodiment the transaction completion system may include a merchant system 130 including POS device 110 in communication with RFID reader 104 (via data link 122). As described more fully below, the transaction completion system may include user interface 134 connected to a network 136 and to the transponder via a USB connector 132.

[0039] Although the point of interaction device may be described herein with respect to a merchant point-of-sale (POS) device, the invention may be not to be so limited. Indeed, a merchant POS device may be used herein by way of example, and the point of interaction device may be any device capable of receiving fob account data. In this regard, the POS may be any point of interaction device enabling the user to complete a transaction using fob 102.

POS device 110 may be in further communication with a customer interface 118 (via data link 128) for entering customer identity verification information. In addition, POS device 110 may be in communication with merchant host network 112 (via data link 124), an issuer host network, and/or any other access point for processing any transaction request. In this arrangement, information provided by RFID reader 104 may be provided to POS device 110 of merchant system 130 via data link 122. POS device 110 may receive the information (and alternatively may receive any identity verifying information from customer interface 118 via data link 128) and provide the information to host system 112 for processing.

[0040] A variety of conventional communications media and protocols may be used for data links 120, 122, 124, and 128. For example, data links 120, 122, 124, and 128 may be an Internet Service Provider (ISP) configured to facilitate communications over a local loop as may be 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 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. Such communications lines are described in a variety of texts, such as, "Understanding Data Communications," by Gilbert Held, which may be incorporated herein by reference.

[0041] An account number, as used herein, may include any identifier for an account (*e.g.*, credit, charge debit, checking, savings, reward, loyalty, travel or the like) which may be maintained by a transaction account provider (*e.g.*, payment authorization center) and which may be used to complete a financial transaction. A typical account number (*e.g.*, account data) may be correlated to a credit or debit account, loyalty account, travel or rewards account maintained and serviced by such entities as American Express, Visa and/or MasterCard, or the like. For ease in understanding, the present invention may be described with respect to a credit card account. However, it should be noted that the invention may be

not so limited and other accounts permitting an exchange of goods and services for an account data value may be contemplated to be within the scope of the present invention.

[0042] In addition, the account number (*e.g.*, account data) may be associated with any device, code, or other identifier/indicia suitably configured to allow the consumer to interact or communicate with the system, such as, for example, authorization/access code, personal identification number (PIN), Internet code, digital certificate, biometric data, and/or other identification indicia. The account number may be optionally located on a rewards card, charge card, credit card, debit card, prepaid card, telephone card, smart card, magnetic stripe card, bar code card, and/or the like. The account number may be distributed and stored in any form of plastic, electronic, magnetic, and/or optical device capable of transmitting or downloading data to a second device. A customer account number may be, for example, a sixteen-digit credit card number, although each credit provider has its own numbering system, such as the fifteen-digit numbering system used by American Express. Each company's credit card numbers comply with that company's standardized format such that the company using a sixteen-digit format will generally use four spaced sets of numbers, as represented by the number "0000 0000 0000 0000". In a typical example, the first five to seven digits are reserved for processing purposes and identify the issuing bank, card type and etc. In this example, the last sixteenth digit may be used as a sum check for the sixteen-digit number. The intermediary eight-to-ten digits are used to uniquely identify the customer. The account number stored as Track 1 and Track 2 data as defined in ISO/IEC 7813, and further may be made unique to fob 102. Track 1 and Track 2 data may be described in more detail below. In one exemplary embodiment, the account number may include a unique fob serial number and user identification number, as well as specific application applets. The account number may be stored in fob 102 inside a database 214, as described more fully below. Database 214 may be configured to store multiple account numbers issued to fob 102 user by the same or different account providing institutions. Where the account data corresponds to a

loyalty or rewards account, database 214 may be configured to store the attendant loyalty or rewards points data.

[0043] FIG. 2 illustrates a block diagram of the many functional blocks of exemplary fob 102 in accordance with the present invention. Fob 102 may be an RFID fob 102 which may be presented by the user to facilitate an exchange of funds or points, etc., for receipt of goods or services. As described herein, by way of example, fob 102 may be an RFID fob which may be presented for facilitating payment for goods and/or services.

[0044] Fob 102 may include an antenna 202 for receiving an interrogation signal from RFID reader 104 via antenna 106 (or alternatively, via external antenna 108). Fob antenna 202 may be in communication with a transponder 114. In one exemplary embodiment, transponder 114 may be a 13.56 MHz transponder compliant with the ISO/IEC 14443 standard, and antenna 202 may be of the 13 MHz variety. Transponder 114 may be in communication with a transponder compatible modulator/demodulator 206 configured to receive the signal from transponder 114 and configured to modulate the signal into a format readable by ahy 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 114 for transmitting to RFID reader 104 via antenna 202. For example, where transponder 114 may be of the 13.56 MHz variety, modulator/demodulator 206 may be ISO/IEC 14443-2 compliant.

[0045] 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 fob 102 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 fob 102 inner-circuitry. For example, protocol/sequence controller 208 may be configured to determine whether the signal provided by RFID reader 104 may be authenticated, and thereby providing to RFID reader 104 the account number stored on fob 102.

[0046] 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 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 may be, in one embodiment, the same. However, data tables having similar, though not identical, data in the key fields may also be merged by using AGREP, for example.

[0047] The data 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 may authenticate the signal provided by RFID reader 104 by association of the RFID signal

to authentication keys stored on database 212. Encryption circuitry may use keys stored on database 212 to perform encryption and/or decryption of signals sent to or from RFID reader 104.

[0048] In addition, protocol/sequence controller 208 may be in communication with a database 214 for storing at least fob 102 account data, and a unique fob 102 identification code. Protocol/sequence controller 208 may be configured to retrieve the account number from database 214 as desired. Database 214 may be of the same configuration as database 212 described above. The fob account data and/or unique fob identification code stored on database 214 may be encrypted prior to storage. Thus, where protocol/sequence controller 208 retrieves the account data, and or unique fob identification code from database 214, the account number may be encrypted when being provided to RFID reader 104. Further, the data stored on database 214 may include, for example, an unencrypted unique fob 102 identification code, a user identification, Track 1 and 2 data, as well as specific application applets.

[0049] In accordance with another exemplary embodiment, the account number may be stored in magnetic stripe format. For example, where the account number may be in magnetic stripe format, the International Standards Organization ISO/IEC 7811, et al. standard, governs the account number portions which are hereby incorporated by reference. The standard requires the magnetic stripe information to be encoded in three "tracks" (*i.e.*, track 1, track 2, and track 3).

[0050] Data stored in track 1 may be typically used to verify the user's identity. Track 1 may be reserved for encoding the transaction account identifier, the name of the accountholder, and at least the expiration date of the transaction account or the transaction device. The information encoded in track 1 may be alpha-numeric and may be encoded at about 7 Bits/Character. In an exemplary layout of the data stored in track 1, track 1 may be segmented into several distinct predetermined portions (*e.g.*, "fields") for encoding the

various account identifying information. The following table may be useful for determining the field definitions of the information provided.

Table of Field Codes for Track 1

SS=Start Sentinel "%"
FC=Format Code
PAN=Primary Acct. # (19 digits max)
FS=Field Separator "^"
Name=26 alphanumeric characters max.
Additional Data=Expiration Date, offset, encrypted PIN, etc.
ES=End Sentinel "?"
LRC=Longitudinal Redundancy Check

Table 1.

[0051] Track 2 may be the track most commonly used by the American Banking Association associated banking institutions. Track 2 may be typically reserved for a duplicate version of the transaction account identifier and the expiration date of the transaction account or the transaction device stored in track 1. In addition, track 2 may include an encrypted Personal Identification Code, and other discretionary data. However, the data in track 2 may be encoded at a lower Bit per Character density than the data encoded in track 1. The data in track 2 may be numeric only and may be encoded at about 5 Bits/Character. The lower density ratio in track 2 may be designed to ensure compatibility with older technology readers and to provide redundancy when reading with newer technology readers. FIG. 8 illustrates an exemplary layout of the data stored in track 2, wherein track 2 may be segmented into several distinct predetermined portions for encoding the various account identifying information. As shown, the following table may be useful for determining the definitions of the information provided.

Table of Field Codes for Track 2

SS=Start Sentinel "%"
SS=Start Sentinel ";"
PAN=Primary Acct. # (19 digits max)
FS=Field Separator "="
Additional Data=Expiration Date, offset, encrypted PIN, etc.

ES=End Sentinel "?"
LRC=Longitudinal Redundancy Check

Table 2.

[0052] Track 3 may be of similar description as Track 2. With the International Standards Organization adoption of standard ISO/IEC 4909, track 3 of the magnetic stripe format was no longer used by the banking industry. However, other transaction devices including a magnetic stripe, such as drivers licenses, use track 3, which may include both numeric only and alpha numeric characters. Track 3 may be unique in that track 3 was intended to have data read and WRITTEN on it. Fob users may have account information UPDATED right on the magnetic stripe. The present invention anticipates that a fob user's travel-related information profile and/or account information may be updated using track 3. Unfortunately, track 3 may be almost an orphaned standard, since most readers currently in operation are not configured to write data onto a magnetic stripe. The original design of track 3 was to control off-line ATM transactions by recording transaction data for later reference by the banking institution. But since ATMs are now on-line, the usage of track 3 has been drastically reduced.

[0053] The most common technique used to encode data in magnetic stripe format may be known as Aiken Biphase, or "two-frequency coherent-phase encoding." The American National Standards Institute (ANSI) and the International Standards Organization (ISO) have chosen two standards to guide the encoding process. The ISO encoding protocol specifies that each of tracks 1, 2 and 3 must begin and end with a length of all Zero bits, called CLOCKING BITS. These are used to synch the self-clocking feature of bi-phase decoding. In addition, most transaction devices which use magnetic stripe encoding protocol use either the ANSI/ISO ALPHA Data format or the ANSI/ISO BCD Data format. For example, track 1 may be typically encoded in ANSI/ISO ALPHA Data format which may be a 7 bit, 6 data bits + 1 parity bit (odd) format, where the data may be read least significant bit first. The ANSI/ISO ALPHA format character set contains 64 characters, 43 alphanumeric, 3

framing/field characters and 18 control/special characters. On the other hand, tracks 2 and 3 are typically encoded in ANSI/ISO BCD Data format, which may be a 5 bit, 4 data bits + 1 parity bit (odd) format. The character set for the ANSI/ISO BCD Data format character set contains 16 characters, 10 alphanumeric, 3 framing/field characters and 3 control/special characters.

[0054] Ordinarily, a proxy account number (*e.g.*, a portion of the transaction account number) includes essential identifying information, such as, for example, any information that may be common to the account provider. The common information (also called "common character," herein) may include the account provider routing number, or common source indicator such as the character spaces reserved to indicate the identification of the issuing bank. Thus, where the proxy transaction account identifier corresponds to an American Express account, the proxy transaction account identifier may include the common character number 3, encoded the field location where such common character may be ordinarily encoded in traditional magnetic stripe format.

[0055] FIG. 6 illustrates the encoding of which may ordinarily be done by an entity, such as, for example, MasterCard in track 2 format. FIG. 6 shows the encoding of a MasterCard account number 3111 2222 3333 4444 with expiration date 12/99 in traditional track 1 format. Since MasterCard uses the number 3 to identify its transaction accounts, the proxy account identifier will also use the number 3 so that the receiving system (*e.g.*, reader 104 or merchant system 130, or account provider) further recognizes that the proxy account identifier may be from a MasterCard transaction device. It should be noted that in this example, the "3" and the "101" may be common characters to all MasterCard transaction accounts. For a more detailed explanation of magnetic stripe format data exchange, see U.S. Patent Application No. 10/810,473, filed on March 26, 2004, entitled "SYSTEM AND METHOD FOR ENCODING INFORMATION IN MAGNETIC STRIPE FORMAT FOR USE IN RADIO FREQUENCY IDENTIFICATION TRANSACTIONS," incorporated herein by reference.

[0056] Fob 102 may be configured to respond to multiple interrogation frequency transmissions provided by RFID reader 104. That may be, as described more fully below, RFID reader 104 may provide more than one RF interrogation signal. In this case, fob 102 may be configured to respond to the multiple frequencies by including in fob 102 one or more additional RF signal receiving/transmitting units 226. RF signal receiving/transmitting unit 226 may include an antenna 218 and transponder 220 where the antenna 218 and transponder 220 are compatible with at least one of the additional RF signals provided by RFID reader 104. For example, in one exemplary embodiment, fob 102 may include a 134 kHz antenna 218 configured to communicate with a 134 kHz transponder 220. In this exemplary configuration, an ISO/IEC 14443-2 compliant modulator/demodulator may not be required. Instead, the 134 kHz transponder may be configured to communicate directly with the protocol/sequence controller 208 for transmission and receipt of authentication and account number signals as described above.

[0057] In another embodiment, fob 102 may further include a universal serial bus (USB) connector 132 for interfacing fob 102 to a user interface 134. User interface 134 may be further in communication with a POS device 110 via a network 136. Network 136 may be the Internet, an intranet, or the like as may be described above with respect to network 112. Further, user interface 134 may be similar in construction to any conventional input devices and/or computing systems aforementioned for permitting the system user to interact with the system. In one exemplary embodiment, fob 102 may be configured to facilitate online Internet payments. A USB converter 222 may be in communication with a USB connector 132 for facilitating the transfer of information between the modulator/demodulator 206 and USB connector 132. Alternatively, USB converter 222 may be in communication with protocol/sequence controller 208 to facilitate the transfer of information between protocol/sequence controller 208 and USB connector 132.

[0058] Where fob 102 includes a USB connector 132, fob 102 may be in communication with, for example, a USB port on user interface 134. The information retrieved from fob 102

may be compatible with credit card and/or smart card technology enabling usage of interactive applications on the Internet. No RFID reader may be required in this embodiment since the connection to POS device 110 may be made using a USB port on user interface 134 and a network 136.

[0059] Fob 102 may include means for enabling activation of the fob by the user. In one exemplary embodiment, a switch 230 which may be operated by the user of fob 102. The switch 230 on fob 102 may be used to selectively or inclusively activate fob 102 for particular uses. In this context, the term "selectively" may mean that the switch 230 enables the user to place fob 102 in a particular operational mode. For example, the user may place fob 102 in a mode for enabling purchase of a good or of a service using a selected account number. Alternatively, the fob may be placed in a mode as such that the fob account number may be provided by USB port 132 (or serial port) only and the fob transponder 114 may be disabled. In addition, the term "inclusively" may mean that fob 102 may be placed in an operational mode permitting fob 102 to be responsive to the RF interrogation and interrogation via the USB connector 132. In one particular embodiment, the switch 230 may remain in an OFF position ensuring that one or more applications or accounts associated with fob 102 are non-reactive to any commands issued by RFID reader 104. As used herein, the OFF position may be termed the "normal" position of the activation switch 230, although other normal positions are contemplated.

[0060] In another exemplary embodiment, when the switch 230 may be moved from the OFF position, fob 102 may be deemed activated by the user. That may be, the switch 230 may activate internal circuitry in fob 102 for permitting the fob to be responsive to RF signals (*e.g.*, commands from RFID reader 104). In this way, switch 230 may facilitate control of the active and inactive states of fob 102. Such control increases the system security by preventing inadvertent or illegal use of fob 102.

[0061] In one exemplary embodiment, switch 230 may be a simple mechanical device in communication with circuitry which may electrically prevent the fob from being powered by

a RFID reader. That may be, when switch 230 may be in its normal position, switch 230 may provide a short to fob 102 internal circuitry, preventing fob 102 from being responsive to interrogation by RF or via the USB connector 230. In this arrangement, the switch 230 may be, for example, a "normally closed" (NC) configured switch, which may be electrically connected to the antenna 202 at the interface of the antenna 202 and the transponder 114. The switch 230 may be depressed, which may open the switch 230 fully activating the antenna 202.

[0062] In yet another exemplary embodiment, fob 102 may include a biometric sensor and biometric membrane configured to operate as switch 230 and activate fob 102 when provided biometric signal from fob 102 user. Such biometric signal may be the digital reading of a fingerprint, thumbprint, or the like. Typically, where biometric circuitry may be used, the biometric circuitry may be powered by an internal voltage source (*e.g.*, battery). In this case, the switch may not be a simple mechanical device, but a switch which may be powered. In yet another exemplary embodiment, switch 230 may be battery powered though no biometric circuitry may be present in fob 102.

[0063] In yet another embodiment, the switch 230 may be a logic switch. Where switch 230 may be a logic switch the switch 230 control software may be read from the sequence controller 208 to selectively control the activation of the various fob 102 components.

[0064] FIG. 3 illustrates an exemplary block diagram of RFID reader 104 in accordance with an exemplary embodiment of the present invention. RFID reader 104 includes, for example, an antenna 202 coupled to a RF module 302, which may be further coupled to a control module 304. In addition, RFID reader 104 may include an antenna 108 positioned remotely from RFID reader 104 and coupled to RFID reader 104 via a suitable cable 120, or other wire or wireless connection.

[0065] RF module 302 and antenna 202 may be suitably configured to facilitate communication with fob 102. Where fob 102 may be formatted to receive a signal at a particular RF frequency, RF module 302 may be configured to provide an interrogation

signal at that same frequency. For example, in one exemplary embodiment, fob 102 may be configured to respond to an interrogation signal of about 13.56 MHz. In this case, RFID antenna 202 may be 13 MHz and may be configured to transmit an interrogation signal of about 13.56 MHz. Fob 102 may be configured to include a first and second RF module (*e.g.*, transponder) where the first module may operate using a 134 kHz frequency and the second RF module may operate using a 13.56 MHz frequency. RFID reader 104 may include two receivers which may operate using the 134 kHz frequency, the 13.56 MHz frequency or both. When the reader 104 may be operating at 134 kHz frequency, only operation with the 134 kHz module on fob 102 may be possible. When the reader 104 may be operating at the 13.56 MHz frequency, only operation with the 13.56 MHz module on fob 102 may be possible. Where the reader 104 supports both a 134 kHz frequency and a 13.56 MHz RF module, fob 102 may receive both signals from the reader 104. In this case, fob 102 may be configured to prioritize selection of the one or the other frequency and reject the remaining frequency. Alternatively, the reader 104 may receive signals at both frequencies from the fob upon interrogation. In this case, the reader 104 may be configured to prioritize selection of one or the other frequency and reject the remaining frequency.

[0066] Further, protocol/sequence controller 314 may include an optional feedback function for notifying the user of the status of a particular transaction. For example, the optional feedback may be in the form of an LED, LED screen and/or other visual display which may be configured to light up or display a static, scrolling, flashing and/or other message and/or signal to inform fob 102 user that the transaction may be initiated (*e.g.*, fob may be being interrogated), the fob may be valid (*e.g.*, fob may be authenticated), transaction may be being processed, (*e.g.*, fob account number may be being read by RFID reader) and/or the transaction may be accepted or denied (*e.g.*, transaction approved or disapproved). Such an optional feedback may or may not be accompanied by an audible indicator (or may present the audible indicator singly) for informing fob 102 user of the transaction status. The audible feedback may be a simple tone, multiple tones, musical indicator, and/or voice indicator

configured to signify when fob 102 may be being interrogated, the transaction status, or the like.

[0067] RFID antenna 202 may be in communication with a transponder 306 for transmitting an interrogation signal and receiving at least one of an authentication request signal and/or an account data from fob 102. Transponder 306 may be of similar description as transponder 114 of FIG. 2. In particular, transponder 306 may be configured to send and/or receive RF signals in a format compatible with antenna 202 in similar manner as was described with respect to fob transponder 114. For example, where transponder 306 may be 13.56 MHz RF rated antenna 202 may be 13.56 MHz compatible. Similarly, where transponder 306 may be ISO/IEC 14443 rated, antenna 202 may be ISO/IEC 14443 compatible.

[0068] RF module 302 may include, for example, transponder 306 in communication with authentication circuitry 308 which may be in communication with a secure database 310. Authentication circuitry 308 and database 310 may be of similar description and operation as described with respect to authentication circuitry 210 and secure memory database 212 of FIG. 2. For example, database 310 may store data corresponding to fob 102 which are authorized to transact business over system 100. Database 310 may additionally store RFID reader 104 identifying information for providing to fob 102 for use in authenticating whether RFID reader 104 may be authorized to be provided the fob account number stored on fob database 214.

[0069] Authentication circuitry 308 may be of similar description and operation as authentication circuitry 210. That may be, authentication circuitry 308 may be configured to authenticate the signal provided by fob 102 in similar manner that authentication circuitry 210 may be configured to authenticate the signal provided by RFID reader 104. As may be described more fully below, fob 102 and 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 fob 102 authenticates the signal from RFID reader 104, and RFID reader 104 authenticates the signal from fob 102.

[0070] FIG. 4 may be a flowchart of an exemplary authentication process in accordance with the present invention. The authentication process may be depicted as one-sided. The flowchart depicts the process of RFID reader 104 authenticating fob 102, although similar steps may be followed in the instance that fob 102 authenticates RFID reader 104.

[0071] As noted, database 212 may store security keys for encrypting or decrypting signals received from RFID reader 104. In an exemplary authentication process, where RFID reader 104 may be authenticating fob 102, RFID reader 104 may provide an interrogation signal to fob 102 (step 402). The interrogation signal may include a random code generated by the RFID reader authentication circuit 210, which may be provided to fob 102 and which may be encrypted using a unique encryption key corresponding to fob 102 unique identification code. For example, the protocol/sequence controller 314 may provide a command to activate the authentication circuitry 308. Authentication circuitry 308 may provide from database 310 a fob 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 may be recognizable (*e.g.*, readable) by RFID reader 104 and fob 102. The authentication code may be provided to fob 102 via the RFID RF interface 306 and antenna 202 (or alternatively antenna 108).

[0072] Fob 102 may receive the interrogation signal (step 404). The interrogation signal including the authorization code may be received at the RF interface 114 via antenna 202. Once fob 102 may be activated, the interrogation signal, including 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 fob 102, and provide the authentication code to authentication circuit 210. Fob 102 may then encrypt the authentication code (step 406). In particular, encryption may be done by authentication circuit 210, which may receive the authentication code and encrypt the code prior to providing the encrypted authentication code to protocol/sequence controller

208. Fob 102 may then provide the encrypted authentication code to RFID reader 104 (step 408). The encrypted authentication code may be provided to RFID reader 104 via modulator/demodulator circuit 206, RF interface 114 (*e.g.*, transponder 114) and antenna 202.

[0073] RFID reader 104 may then receive the encrypted authentication code and decrypt it (step 410). The encrypted authentication code may be received at antenna 202 and RF interface 306 and may be provided to authentication circuit 308. Authentication circuit 308 may be provided a security authentication key (*e.g.*, transponder system decryption key) from database 310. The authentication circuit may use the authentication key to decrypt (*e.g.*, unlock) the encrypted authorization code. The authentication key may be provided to the authentication circuit based on fob 102 unique identification code. For example, the encrypted authentication code may be provided along with the unique fob 102 identification code. The authentication circuit may receive fob 102 unique identification code and retrieve from the database 310 a transponder system decryption key correlative to the unique fob 102 identification code for use in decrypting the encrypted authentication code.

[0074] Once the authentication code may be decrypted, the decrypted authentication code may be compared to the authentication code provided by RFID reader 104 at step 402 (step 412) to verify its authenticity. If the decrypted authorization code is not readable (*e.g.*, recognizable) by the authentication circuit 308, fob 102 may be deemed to be unauthorized (*e.g.*, unverified) (step 418) and the operation of system 100 may be terminated (step 420). Contrarily, if the decrypted authorization code may be recognizable (*e.g.*, verified) by fob 102, the decrypted authorization code may be deemed to be authenticated (step 414), and the transaction may be allowed to proceed (step 416). In one particular embodiment, the preceding transaction may mean that fob 102 may authenticate RFID reader 104, although, it should be apparent that RFID reader 104 may authenticate fob 102 prior to fob 102 authenticating RFID reader 104.

[0075] It should be noted that in an exemplary verification process, the authorization circuit 308 may determine whether the unlocked authorization code may be identical to the authorization code provided in step 402. If the codes are not identical then fob 102 may not be authorized to access system 100. Although, the verification process may be described with respect to identicality, identicality may be not required. For example, authentication circuit 308 may verify the decrypted code through any protocol, steps, or process for determining whether the decrypted code corresponds to an authorized fob 102.

[0076] Authentication circuitry 308 may additionally be in communication with a protocol/sequence controller 314 of similar operation and description as protocol/sequence controller 208 of FIG. 2. That may be, protocol/sequence device controller 314 may be configured to determine the order of operation of RFID reader 104 components. For example, FIG. 5 illustrates an exemplary decision process under which protocol/sequence controller 314 may operate. Protocol/sequence controller 314 may command the different components of RFID reader 104 based on whether fob 102 may be present (step 502). For example, if fob 102 may not be present, then protocol/sequence controller 314 may command RFID reader 104 to provide an uninterrupted interrogation signal (step 504). The protocol/sequence controller may command the authentication circuit 308 to provide an uninterrupted interrogation signal until the presence of fob 102 may be realized. If fob 102 may be present, the protocol/sequence controller 314 may command RFID reader 104 to authenticate fob 102 (step 506).

[0077] As noted above, authentication may mean that the protocol/sequence controller 314 may command the authentication circuit 308 to provide fob 102 with an authorization code. If a response may be received from fob 102, protocol/sequence controller may determine if the response may be a response to RFID reader 104 provided authentication code, or if the response may be a signal requiring authentication (step 508). If the signal requires authentication, then the protocol/sequence controller 314 may activate the authentication circuit as described above (step 506). On the other hand, if fob 102 signal may be a response

to the provided authentication code, then the protocol/sequence controller 314 may command RFID reader 104 to retrieve the appropriate security key for enabling recognition of the signal (step 510). The protocol/sequence controller 314 may command the authentication circuit 308 to retrieve from database 310 a security key (*e.g.*, transponder system decryption key), unlock the signal, and compare the signal to the signal provided by RFID reader 104 in the authentication process (*e.g.*, step 506). If the signal is recognized, the protocol/sequence controller 314 may determine that fob 102 may be authorized to access the system 100. If the signal is not recognized, then the fob may be considered not authorized, in which case, protocol/sequence controller 314 may command the RFID controller to interrogate for authorized fobs (step 504).

[0078] Once the protocol/sequence controller determines that fob 102 may be authorized, the protocol/sequence controller 314 may seek to determine if additional signals are being sent by fob 102 (step 514). If no additional signal may be provided by fob 102, then the protocol/sequence controller 314 may provide all the components of RFID reader 104 to remain idle until such time as a signal may be provided (step 516). Contrarily, where an additional fob 102 signal may be provided, the protocol/sequence controller 314 may determine if fob 102 may be requesting access to the merchant point-of-sale terminal 110 (*e.g.*, POS device) or if fob 102 may be attempting to interrogate RFID reader 104 for return (*e.g.*, mutual) authorization (step 518). Where fob 102 may be requesting access to a merchant POS device 110, the protocol/sequence controller 314 may command the RFID reader to open communications with the POS device 110 (step 524). In particular, the protocol/sequence controller may command the POS device 110 communications interface 312 to become active, permitting transfer of data between RFID reader 104 and the merchant POS device 110.

[0079] On the other hand, if the protocol/sequence controller determines that fob 102 signal may be a mutual interrogation signal, then the protocol/sequence controller may command RFID reader 104 to encrypt the signal (step 520). The protocol/sequence controller 314 may

command the encryption authentication circuit 318 to retrieve from database 320 the appropriate encryption key in response to fob 102 mutual interrogation signal. The protocol/sequence controller 314 may then command RFID reader 104 to provide the encrypted mutual interrogation signal to fob 102. The protocol/sequence controller 314 may command the authentication circuit 318 to provide an encrypted mutual interrogation signal for fob 102 to mutually authenticate. Fob 102 may then receive the encrypted mutual interrogation signal and retrieve from authentication circuitry 212 a RFID reader decryption key.

[0080] Although an exemplary decision process of protocol/sequence controller 314 may be described, it should be understood that a similar decision process may be undertaken by protocol/sequence controller 208 in controlling the components of fob 102. Indeed, as described above, protocol/sequence controller 314 may have similar operation and design as protocol/sequence controller 208. In addition, to the above, protocol/sequence controllers 208 and 314 may incorporate in the decision process appropriate commands for enabling USB interfaces 222 and 316, when the corresponding device may be so connected.

[0081] Encryption/decryption component 318 may be further in communication with a secure account number database 320 which stores the security keys for decrypting the encrypted fob account number. Upon appropriate request from protocol/sequence controller 314, encryption/decryption component (*e.g.*, circuitry 318) may retrieve the appropriate security key, decrypt the fob account number and forward the decrypted account number to protocol sequence controller 314 in any format readable by any later connected POS device 110. In one exemplary embodiment, the account number may be forwarded in a conventional magnetic stripe format compatible with the ISO/IEC 7813 standard. Upon receiving the account number in magnetic stripe format, protocol/sequence controller 314 may forward the account number to POS device 110 via a communications interface 312 and data link 122, as best shown in FIG. 1. POS device 110 may receive the decrypted account number and forward the magnetic stripe formatted account number to a merchant network

112 for processing under the merchant's business as usual standard. In this way, the present invention eliminates the need of a third-party server. Further, where POS device 110 may receive a response from network 112 (*e.g.*, transaction authorized or denied), protocol/sequence controller 314 may provide the network response to the RF module 302 for optically and/or audibly communicating the response to fob 102 user.

[0082] RFID reader 104 may additionally include a USB interface 316, in communication with the protocol/sequence controller 314. In one embodiment, the USB interface may be a RS22 serial data interface. Alternatively, RFID reader 104 may include a serial interface such as, for example, a RS232 interface in communication with the protocol/sequence controller 314. The USB connector 316 may be in communication with a personalization system 116 (shown in FIG. 18) for initializing RFID reader 104 to system 100 application parameters. Prior to operation of system 100, RFID reader 104 may be in communication with personalization system 116 for populating database 310 with a listing of security keys belonging to authorized fobs 102, and for populating database 320 with the security keys to decrypt fob 102 account numbers placing the account numbers in ISO/IEC 7813 format. In this way, RFID reader 104 may be populated with a unique identifier (*e.g.*, serial number) which may be used by fob authentication circuitry 210 to determine if RFID reader 104 may be authorized to receive fob 102 encrypted account number.

[0083] FIG. 8 illustrates an exemplary flow diagram for the operation of system 100. The operation may be understood with reference to FIG. 1, which depicts the elements of system 100 which may be used in an exemplary transaction. The process may be initiated when a customer desires to present fob 102 for payment (step 802). Upon presentation of fob 102, the merchant initiates the RF payment procedure via an RFID reader 104 (step 804). In particular, the RFID reader sends out an interrogation signal to scan for the presence of fob 102 (step 806). The RF signal may be provided via the RFID reader antenna 106 or optionally via an external antenna 108. The customer may then present fob 102 for payment (step 808) and fob 102 may be activated by the RF interrogation signal provided

[0084] Fob 102 and RFID reader 104 may then engage in mutual authentication (step 810). Where the mutual authentication may be unsuccessful, an error message may be provided to the customer via the RFID optical and/or audible indicator (step 814) and the transaction may be aborted (step 816). Where the mutual authentication may be successful (step 814), RFID reader 104 may provide the customer with an appropriate optical and/or audible message (*e.g.*, "transaction processing" or "wait") (step 818). The fob protocol/sequence controller 208 may then retrieve from database 214 an encrypted fob account number and provide the encrypted account number to RFID reader 104 (step 820).

[0085] RFID reader 104 may then decrypt the account number and convert the account number into magnetic stripe (ISO/IEC 7813) format (step 822) and provide the unencrypted account number to the merchant system 130 (step 828). In particular, the account number may be provided to POS device 110 for transmission to the merchant network 112 for processing under known business transaction standards. POS device 110 may then send an optical and/or audible transaction status message to RFID reader 104 (step 830) for communication to the customer (step 832) and the transaction is completed (step 834).

[0086] It should be noted that the transaction account associated with fob 102 may include a restriction, such as, for example, a per purchase spending limit, a time of day use, a day of week use, certain merchant use and/or the like, wherein an additional verification may be required when using the fob outside of the restriction. The restrictions may be personally assigned by fob 102 user, or the account provider. For example, in one exemplary embodiment, the account may be established such that purchases above $X (*i.e.*, the spending limit) must be verified by the customer. Such verification may be provided using a suitable PIN which may be recognized by RFID reader 104 or a payment authorization center (not shown) as being unique to fob 102 holder (*e.g.*, customer) and the correlative fob 102 transaction account number. Where the requested purchase may be above the established per purchase spending limit, the customer may be required to provide, for example, a PIN, biometric sample and/or similar secondary verification to complete the transaction.

[0087] Where a verification PIN may be used as secondary verification the verification PIN may be checked for accuracy against a corroborating PIN which correlates to fob 102 transaction account number and/or the fob user's travel-related information. The corroborating PIN may be stored locally (*e.g.*, on fob 102, or on RFID reader 104) or may be stored on a database (not shown) at the payment authorization center. The payment authorization center database may be any database maintained and operated by fob 102 transaction account provider.

[0088] The verification PIN may be provided to POS device 110 using a conventional merchant (*e.g.*, POS) PIN key pad 118 in communication with POS device 110 as shown in FIG. 1, or a RFID keypad in communication with RFID reader 104. PIN keypad may be in communication with POS device 110 (or alternatively, RFID reader 104) using any conventional data link described above. Upon receiving the verification PIN, RFID reader 104 may seek to match the PIN to the corroborating PIN stored on RFID reader 104 at database 310 or 320. Alternatively, the verification PIN may be provided to a payment authorization center to determine whether the PIN matches the PIN stored on the payment authorization center database which correlates to fob 102 account. If a match may be made, the purchase may no longer be restricted, and the transaction may be allowed to be completed.

[0089] In another exemplary embodiment of the present invention, system 100 may be configured with one or more biometric scanners, processors and/or systems. A biometric system may include one or more technologies, or any portion thereof, such as, for example, recognition of a biometric. As used herein, a biometric may include a user's voice, fingerprint, facial, ear, signature, vascular patterns, DNA sampling, hand geometry, sound, olfactory, keystroke/typing, iris, retinal or any other biometric relating to recognition based upon any body part, function, system, attribute and/or other characteristic, or any portion thereof. While the example discussed herein may include a particular biometric system or

sample, the invention contemplates any of the biometrics discussed herein in any of the embodiments.

[0090] The biometric system may be configured as a security system and may include a registration procedure in which a user of transaction instrument (*e.g.*, fob 102) proffers a sample of his fingerprints, DNA, retinal scan, voice, and/or other biometric sample to an authorized sample receiver (ASR). An ASR may include a local database, a remote database, a portable storage device, a host system, an issuer system, a merchant system, a fob issuer system, an employer, a financial institution, a non-financial institution, a loyalty point provider, a company, the military, the government, a school, a travel entity, a transportation authority, a security company, and/or any other system or entity that is authorized to receive and store biometric samples and associate the samples with specific biometric databases and/or transaction instruments (*e.g.*, fobs 102). As used herein, a user of a fob, fob user, or any similar phrase may include the person or device holding or in possession of the fob, or it may include any person or device that accompanies or authorizes the fob owner to use the fob. By proffering one or more biometric samples, a biometric may be scanned by at least one of a retinal scan, iris scan, fingerprint scan, hand print scan, hand geometry scan, voice print scan, vascular scan, facial and/or ear scan, signature scan, keystroke scan, olfactory scan, auditory emissions scan, DNA scan, and/or any other type of scan to obtain a biometric sample.

[0091] Upon scanning the sample, the system may submit the scanned sample to the ASR in portions during the scan, upon completing the scan or in batch mode after a certain time period. The scanned sample may include a hardcopy (*e.g.*, photograph), digital representation, an analog version or any other configuration for transmitting the sample. The ASR may receive the sample and the ASR may also receive copies of a fob user's biometric data along with the sample or at a different time (or within a different data packet) from receiving the sample.

[0092] The ASR and/or fob user 102 may store the sample in digital and/or any storage medium known in the art and correlate and/or register the sample with fob user information. By storing the sample in digital format, the ASR may digitize any information contained in one of the biometric scans described herein. By storing the sample in any storage medium, the ASR may print and/or store any biometric sample. Hardcopy storage may be desirable for back-up and archival purposes. As used herein, registered samples may include samples that have been proffered, stored and associated with user information.

[0093] The biometric sample may also be associated with user information. The sample may be associated with user information at any step in the process such as, for example, prior to submission, during submission and/or after submission. In one embodiment, the user may input a PIN number or zip code into the POS terminal, then scan the biometric to create the biometric sample. The local POS system may associate the biometric sample data with the PIN and zip code, then transmit the entire packet of information to the ASR. In another embodiment, the POS may facilitate transmitting the sample to an ASR, and during the transmission, the sample may be transmitted through a third system which adds personal information to the sample.

[0094] The information associated with the biometric sample may include any information such as, for example, fob user information, fob 102 information, fob 102 identifier information, fob 102 vender information, fob 102 operability information, and/or fob 102 manufacturing information. Fob 102 information is not limited to transponder information and may include information related to any transaction instrument such as smart fobs, credit fobs, debit fobs, merchant-specific fobs, loyalty point fobs, cash accounts and any other transaction instruments and/or accounts. The fob user information may also contain information about the user including personal information--such as name, address, and contact details; financial information--such as one or more financial accounts associated with the fob user; loyalty point information--such as one or more loyalty point accounts (*e.g.*, airline miles, charge fob loyalty points, frequent diner points) associated with the fob user;

and/or non-financial information--such as employee information, employer information, medical information, family information, and/or other information that may be used in accordance with a fob user.

[0095] For example, fob user may have previously associated a credit card account, a debit card account, and a frequent flier account with his biometric sample which is stored at an ASR. Later, when fob user desires to purchase groceries, fob user may submit his biometric sample while using fob 102 for the purchase at a POS. The POS may facilitate sending the biometric sample to the ASR such that the ASR authorizes the biometric sample and checks a look-up table in the ASR database to determine if any information is associated with the sample. If information (*e.g.*, financial accounts) is associated with the sample, the ASR may transmit the information to the POS terminal. The POS terminal may then present fob user with a list of the three accounts associated with the biometric sample. Fob user and/or a merchant may then choose one of the accounts in order to continue and finalize the transaction.

[0096] The ASR and/or fob user may associate a specific fob 102 identifier with the biometric sample by any method known in the art for associating an identifier (*e.g.*, through the use of software, hardware and/or manual entry). The ASR may additionally verify the fob user and/or fob 102 by using one or more forms of the user's secondary identification. For example, the ASR may verify the fob user by matching the fob information to information retrieved from scanning information from a fob user's driver's license. The ASR may verify fob 102 by contacting the vendor of fob 102 to confirm that fob 102 was issued to a specific fob user. In another embodiment, the ASR may activate fob 102 during the registration procedure to confirm that fob 102 transponder identifier and other information is properly associated with the fob user and the fob user's specific biometric samples. The ASR may additionally employ one or more verification methods to confirm that the biometric sample belongs to the user, such as, for example, the ASR may request from the user demographic information, further biometric samples and/or any other information. As

used herein, "confirm," "confirmation" or any similar term includes verifying or substantially verifying the accuracy, existence, non-existence, corroboration, and/or the like of the information, component, or any portion thereof. The ASR may additionally employ one or more additional processing methods in order to facilitate association of a biometric sample. As used herein, the term processing may include scanning, detecting, associating, digitizing, printing, comparing, storing, encrypting, decrypting, and/or verifying a biometric and/or a biometric sample, or any portion thereof.

[0097] Upon association, authentication and/or verification of the biometric sample and fob 102, the system may store the sample and fob 102 identifier in one or more databases on and/or in communication with system 100 via a network, server, computer, or any other means of communicating as described herein. The database(s) may be any type of database described herein. For example, a biometric sample stored on fob 102 may be stored in database 212. The database(s) may be located at or operated by any of the entities discussed herein such as, for example, the ASR and/or by a third-party biometric database operator.

[0098] The system may further protect the samples by providing additional security with the sample. The security may include, for example, encryption, decryption, security keys, digital certificates, firewalls and/or any other security methods known in the art and discussed herein. One or more security vendors may utilize the security methods to store and/or access the biometric samples. The present invention anticipates that storage of the biometric samples may be such that a sample is first encrypted and/or stored under a security procedure, such that the sample may only be accessed by a vendor with the proper level of access or security which corresponds to or provides access to the stored sample. The samples may be accessible by certain vendors such as, for example, fob 102 transaction account provider system, an issuer system, a merchant system, a fob issuer system, an employer, a financial institution, a non-financial institution, a loyalty-point provider, a company, the military, the government, a school, a travel entity, a transportation authority, and/or a security company.

[0099] The fob of the invention may include a particular security system wherein the security system incorporates a particular biometric system. As shown in FIG. 9, fob 102 may include a biometric security system 902 configured for facilitating biometric security using, for example, fingerprint samples. As used herein, fingerprint samples may include samples of one or more fingerprints, thumbprints, palmprints, footprints, and/or any portion thereof. Biometric security system 902 may include a biometric sensor 904 which may be configured with a sensor and/or other hardware and/or software for acquiring and/or processing the biometric data from the person such as, for example, optical scanning, capacitance scanning, or otherwise sensing the portion of fob user. In one embodiment, biometric sensor 904 of the security system 902 may scan a finger of a fob user in order to acquire his fingerprint characteristics into fob 102. Biometric sensor 904 may be in communication with a sensor interface/driver 906 such that sensor interface 906 may receive the fingerprint information and transmits a signal to controller 208 to facilitate activating the operation of fob 102. A power source (*e.g.*, battery 903) may be in communication with biometric sensor 904 and sensor interface 906 to provide the desired power for operation of the biometric security system components.

[00100] In one exemplary application of fob 102 incorporating biometric security system 902, the user may place his finger on the biometric sensor to initiate the mutual authentication process between fob 102 and RFID reader 104, and/or to provide verification of the user's identity. Fob 102 may digitize the fingerprint and compare it against a digitized fingerprint stored in a database (*e.g.*, security database 212) included on fob 102. The fingerprint information may additionally be compared with information from one or more third-party databases communicating with fob 102 through any communication software and/or hardware, including for example, RFID reader 104, a USB connection, a wireless connection, a computer, a network and/or any other means for communicating. This transfer of information may include use of encryption, decryption, security keys, digital certificates and/or other security devices to confirm the security of the sample. Fob 102 may

additionally communicate with third-party databases to facilitate a comparison between fob 102 identifier and other fob identifiers stored with the biometric samples. As used herein, compare, comparison and similar terms may include determining similarities, differences, existence of elements, non-existence of elements and/or the like.

[00101] Protocol/sequence controller 208 may facilitate the local comparison to authenticate the biometric and authentication circuit 210 may validate the information. Any of the embodiments may alternatively or additionally include remote comparisons performed or controlled by one or more third-party security vendors. One or more comparison techniques and/or technologies may be used for comparisons. For example, for fingerprint comparisons, protocol/sequence controller 208 may utilize an existing database to compare fingerprint minutia such as, for example, ridge endings, bifurcation, lakes or enclosures, short ridges, dots, spurs and crossovers, pore size and location, Henry System categories such as loops, whorls, and arches, and/or any other method known in the art for fingerprint comparisons.

[00102] Fob 102 may additionally be configured with secondary security procedures to confirm that fake biometric samples are not being used. For example, to detect the use of fake fingers, fob 102 may be further configured to measure blood flow, to check for correctly aligned ridges at the edges of the fingers, and/or any other secondary procedure to reduce biometric security fraud. Other security procedures for ensuring the authenticity of biometric samples may include monitoring pupil dilation for retinal and/or iris scans, pressure sensors, blinking sensors, human motion sensors, body heat sensors and/or any other procedures known in the art for authenticating the authenticity of biometric samples.

[00103] After verifying the biometric information, fob 102 and RFID reader 104 may begin mutual authentication, and the transaction may proceed accordingly. However, the invention contemplates that the verification of biometric information may occur at any point in the transaction such as, for example, after the mutual authentication. At any point in the transaction, the system may additionally request fob user to enter a PIN and/or other identifier associated with the transaction account and/or biometric sample to provide further

verification of fob user's identification. As part of the transaction, fob user payer may be requested to select from one of the financial accounts, loyalty accounts, credit accounts, debit account, and/or other accounts associated with the biometric sample. The user may be presented with a list of account options on a display associated with RFID reader 104, fob 102, a third-party security device and/or any other financial or transaction device association with a transaction. In another embodiment, a payee may select one of the accounts. For example, a department store payee may manually and/or automatically select a department store issued account, if available, for a transaction.

[00104] The present invention includes systems and methods for facilitating personalizing and dynamically synchronizing fobs and associated databases in the context of a distributed transaction system. More particularly, referring now to FIG. 10, an exemplary dynamic synchronization system (DSS) may comprise a support client server 1004 (*e.g.*, a secure server), a fob object database update system 1006 (FODUS), one or more enterprise data synchronization interfaces 1008 (EDSI), an update logic system 1010, one or more enterprise data collection units 1012 (EDCUs), and one or more POS devices 110 configured with RFID reader 104 to interoperably accept information from and interface with fobs 102. In an exemplary embodiment, DSS may also suitably comprise a personalization system 116 and an account maintenance system 142 configured to communicate with FODUS 1006.

[00105] More particularly, in an exemplary embodiment, secure support client server 1004 may communicate over a suitable network to EDSIs 1008 through enterprise networks 1014. EDSIs 1008 communicate with update logic system 1010, which itself communicates with enterprise data collection units 1012. Enterprise data collection units 1012 communicate with FODUS 1006 and secure support client server 1004. In general, as described in further detail below, each enterprise (*e.g.*, airline partner, hotel partner, travel agency, etc.) may be associated with a corresponding EDSI 1008, network 11014, and EDCU 1012. That is, EDCU 1012(a) corresponds to EDSI 1008(a) and network 1014(a), EDCU 1012(b) corresponds to EDSI 1008(b) and network 1014(b), and so on. The DSS may include an

arbitrary number of such functional blocks in accordance with the number of enterprises represented.

[00106] Personalization system 116 may suitably function as the issuing source of fobs 102. That is, personalization system 116 facilitates creating and issuing fobs for use by the consumer by providing a predetermined file structure populated with initialization data (*e.g.*, account numbers, serial numbers, default preferences, and the like). In this regard, FODUS 1006 interfaces with personalization system 116 in order to facilitate re-issuance of the fob by providing updated data in the event a fob is destroyed, lost, or stolen. Personalization system 116 is described in detail below in conjunction with FIG. 18.

[00107] Account maintenance system 142 may be provided for customer service purposes and, in this capacity, may act as the point of entry for fob user complaints, questions, and other customer input. FODUS 1006 may suitably communicate with account maintenance system 142 in order to assist customer service representatives and/or automated systems in addressing fob user issues.

Fob POS devices

[00108] POS devices 110 may allow the fob user to gain access to the distributed transactions system through a variety of means. Such POS devices may include, for example, standard home telephones, various PCS wireless systems, pay phones, palmtops computers, notebook computers, Internet workstations, automated teller machines (ATMs), point-of-sale terminals (POS) stand-alone kiosks, network computers (NCs), personal data assistants (PDAs), or any other suitably configured communication apparatus. POS device 110 may be portable (as in the case of PDAs and cellular phones) or centrally located, for example, in airline ticketing and gate areas, rental car facilities, hotel lobbies, travel agencies, and malls. In addition, businesses may host POS device 110 to streamline their employees' business travel. In an exemplary embodiment, various POS devices 110 may be configured to interface with (or incorporate) contactless fobs 102 or fob receivers in accordance with the relevant portions of the ISO-14443 standard.

Secure Support Client Server

[00109] Secure support client server 1004 may provide, where appropriate, any functionality missing from the individual POS devices 110 used during a transaction. Server 1004 also suitably handles routing of messages from POS device 110 to the appropriate EDSI 1008 and/or EDCU 1012.

[00110] Referring now to FIGS. 10 and 11, an exemplary secure support client server 1004 may comprise a security engine 1102, a supplemental application support 1104, and a router 1106. Security engine 1102 may comprise suitable hardware and/or software configured to provide messaging (*e.g.*, secure messaging) between server 1004, EDSUs 1012, and networks 1014. More specifically, security engine 1102 utilizes authentication, data encryption, and digital signature techniques in connection with incoming and outgoing message packets. A variety of conventional security algorithms are suitable in the context of the present invention, including, for example, DES encryption, RSA authentication, and a variety of other symmetrical and non-symmetrical cryptographic techniques.

[00111] Supplemental application support 1104 may comprise suitable hardware and/or software components related to specific POS device 110 functionality. More particularly, server 1004 may suitably determine the nature of POS device 110 utilized during a transaction. If POS device 110 does not include the appropriate software for effecting the requested transaction, then server 1004 supplies the functionality (*i.e.*, software modules) which completes the transaction with respective EDSIs 1008 and/or EDCUs 1012. The supplemental functionality may include, inter alia, software modules for properly formatting message packets (described in further detail below) sent out over the various networks comprising the DSS. For example, where a transaction takes place via POS device 110 which may consist entirely of a stand-alone RFID reader 104, then nearly all functionality may be supplied by server 1004 because RFID reader 104, by itself, may only be capable of transferring messages to and from fob 102 in a "dumb" manner. However, when a suitably configured PC and/or RFID reader 104 is configured with POS device 110, most

functionality may be supplied by various software modules residing in the PC and/or RFID reader 104. In such a case, server 1004 may only transfer the various message packets to and from POS device 110 without supplying additional software. Added functionality may be supplied through any suitable method, for example, through the use of portable software code (*e.g.*, Java, ActiveX, and the like), or distributed software residing within POS device 110, fobs 102, RFID reader 104 and/or server 1004.

[00112] Router 1106 suitably handles routing of messages to the appropriate EDCUs 1012, networks 1014, and POS device 110. That is, router 1106 may be configured to identify the appropriate functional blocks within the DSS to which a given message packet should be sent. The identification of the appropriate functional blocks may take place in a number of ways. In an exemplary embodiment, the identification may be accomplished through the use of a look-up table comprising a list of appropriate destinations keyed to information extracted from requests received from POS device 110.

[00113] In an alternate embodiment, a secure support client server 1004 may not be used, and the functionality of POS devices 110 may be suitably specified in order to obviate the need for server 1004. Alternatively, the functions of server 1004 may be allocated and distributed throughout the DSS components in any advantageous manner.

[00114] It will be appreciated by those skilled in the art that the term "transaction" refers, generally, to any message communicated over the system for effecting a particular goal, for example, travel transaction, financial transaction, debit/charge authorization, preference changes, reservation requests, ticket requests, and the like. FIG. 7, for example, shows an exemplary transaction data structure useful in the context of performing an on-line transaction with a travel partner, wherein the field name 702, data type 704 ('C' for character), maximum byte-length 706, and description 708 are listed in tabular form. In this example, the transaction messages suitably may comprise comma delimited data packets, although other data structures may be employed.

Fob Object Database Update System (FODUS)

00115] FODUS 1006 suitably stores information (*e.g.*, securely stores) related to the state of the various issued fobs 102. Referring now to FIGS. 10 and 15, in an exemplary embodiment, FODUS 1006 may comprise a security engine 1502, a data management module 1504, a fob object database 212, a fob object administration module 1506, and an audit file 1508.

00116] Security engine 1502 may provide suitable security for, inter alia, the information stored within fob object database 212. In this regard, security engine 1502 may utilize various authentication, data encryption, and digital signature techniques in connection with incoming and outgoing message packets. Suitable algorithms in the context of the present invention, include, for example, DES encryption, RSA authentication, and a variety of other symmetrical and non-symmetrical cryptographic techniques.

00117] Data management module 1504 may suitably act as a data interface between FODUS 1006 and account maintenance 142 as well as between FODUS 1006 and the various EDCUs 1012. More specifically, module 604 facilitates converting and translating between the data format used in these systems. For example, data stored within object database 106 may not be stored in a format which may be easily used by EDCUs 1012 or account maintenance 142. Accordingly, data management module 1504 may comprise suitable routines for effecting conversion and formatting of both incoming and outgoing data.

[00118] Fob object administration module 1506 may provide suitable database software to edit, update, delete, synchronize, and ensure substantial non-corruption of data stored within object database 212. A variety of database packages are suitable for this task, including, for example, various conventional fourth-generation relational database management systems (4GL RDBMS).

[00119] Audit file 1508 may suitably track changes to object database 116, thereby helping to ensure the integrity of fob data stored within FODUS 1006. More particularly, when changes to object database 116 take place as a result of preference updates, transactions, application

structure changes, and the like, audit file 1508 may track suitable information related to these changes (*e.g.*, time, date, and nature and content of the change).

[00120] Fob object database 212, which may comprise a single database or a set of distributed databases, may be used to store the known state of the various fobs 102. In general, the state of a fob may be characterized by a suitable set of fob indicia. In an exemplary embodiment, wherein a data structure in accordance with ISO-7816 is employed, fob object database 212 stores information related to the individual applications present on the various fobs 102 (*i.e.*, the overall file structure) as well as the individual fields, directories, and data that may comprise those applications. A file structure for fob object database 212 may be chosen such that it includes a suitable set of data fields for a given fob 102.

Enterprise Data Synchronization Interface

[00121] In an exemplary embodiment, the various EDSIs 1008 may track changes to fob data and/or applications corresponding to individual enterprises. With reference to FIGS. 10 and 12, in an exemplary embodiment, EDSI 1008 may comprise a communication server 1202, a security engine 1204, and a customer database 1206.

[00122] Communication server 1202 may suitably facilitate communication with networks 112 and update logic system 1010. In this regard, server 302 may be configured to translate between various formats, media, and communication protocols as may be necessary or desired given the particular choice of components employed.

[00123] Security engine 1204 may provide suitable security measures with respect to the access and storage of information with customer database 1206. Security engine 1204 may utilize various authentication, data encryption, and digital signature techniques in connection with incoming and outgoing message packets. Suitable algorithms in the context of the present invention, may include, for example, DES encryption, RSA authentication, and a variety of other symmetrical and non-symmetrical cryptographic techniques.

[00124] Customer database 1206 may suitably provide a means for storing fob information related to individual partners or enterprises. That is, a particular enterprise (hosting, for

example, network 112(a)) may compile, or employ others to compile, fob information related only to that enterprise. For example, a hotel chain may store loyalty, preference, and other data that relates specifically to that hotel chain. During synchronization (as described in further detail below) any changes to database 306 may be propagated through the system and, visa-versa, changes elsewhere in the system may be communicated to database 306. This communication may be done securely (using security engine 1204) in conjunction with communication server 1202.

[00125] In an alternate embodiment, the functionality provided by the EDSIs 1008 may be folded into the corresponding EDCU 1012. That is, while an illustrated embodiment may employ one or more physically separate EDSIs 1008, it may be advantageous to further streamline the DSS by incorporating this functionality into the corresponding EDCU 1012 functional block.

Update Logic System

[00126] In an exemplary embodiment, update logic system 1010 may format and securely routes fob data received from and transmitted to EDCUs 1012 and EDSIs 1008. Referring now to FIG. 13, in an exemplary embodiment, update logic system 1010 may include a logic engine 1302, a data management module 1304, a security engine 1306, an enterprise update administrator 1308, and an enterprise update audit module 1310.

[00127] Logic engine 1302 may suitably function to direct and distribute information changes across the system. Thus, logic engine 1302 may be able to determine which modules (*i.e.*, which EDCUs 1012 and EDSIs 1008) need to reflect the change.

[00128] Data management module 1304 may suitably act as a data interface between EDSIs 1008 and EDCUs 1012. More specifically, module 1304 may be able to convert and translate between data format used in these systems. Accordingly, data management module 1304 may comprise suitable routines for effecting conversion and formatting of both incoming and outgoing data.

[00129] Security engine 1306 may be used to provide suitable security measures with respect to data flowing through update logic system 1010. Security engine 1306 may utilize various authentication, data encryption, and digital signature techniques in connection with incoming and outgoing message packets. Suitable algorithms in the context of the present invention, may include, for example, DES encryption, RSA authentication, and a variety of other symmetrical and non-symmetrical cryptographic techniques.

[00130] Enterprise update administrator 1308 may suitably comprise overhead software used to maintain data transfer between EDSIs 1008 and EDCUs 1012.

[00131] Enterprise update audit module 1310 may suitably track updated information flowing through update logic system 1010. More particularly, when information is communicated across update logic system 1010 (as a result of preference updates, transactions, application structure changes, and the like), audit module 1310 may track suitable indicia of this information (*e.g.*, time, date, and nature and content of the communication).

Enterprise Data Collection Unit

[00132] EDCUs 1012 may facilitate storing and coordinating the transfer of synchronization data corresponding to a particular enterprise. With reference to FIG. 14, in an exemplary embodiment, enterprise data collection unit 1012 may include a security engine 1408, a customer update transaction database 1404, a customer loyalty transaction database 1410, a customer pending transaction database 1414, an update database 1402, an EDCU audit file 1406, an EDCU administrative file 1412, and an EDCU data management module 1416.

[00133] Security engine 1408 may be used to provide suitable security measures with respect to data flowing through EDCU 1012. Toward this end, security engine 1408 may utilize various authentication, data encryption, and digital signature techniques in connection with incoming and outgoing message packets. Suitable algorithms in the context of the present invention, may include, for example, DES encryption, RSA authentication, and a variety of other symmetrical and non-symmetrical conventional cryptographic techniques.

[00134] Customer update transaction database 1404 may be used to store information which has been updated on a fob 102, but which has not yet propagated to the various databases and networks that require updating. For example, a fob 102 may be used to change fob user preferences in the course of a transaction with a particular enterprise. This information may, in the short term, be stored in database 1404 (for the particular enterprise) until it could be fanned-out to FODUS 1006 and the appropriate EDCUs 1012 and EDSIs 1008. This type of transaction is described in further detail below.

[00135] Customer loyalty transaction database 1410 may be suitably used to store loyalty information (*e.g.*, frequent flier, frequent stayer, etc.) associated with a particular enterprise or partner. In an alternate embodiment, a loyalty transaction database 1410 may not be employed – rather, the functionality of database 1410 may be incorporated into databases 1402, 1410, and 1414 such that a loyalty transaction becomes just another transaction modality to be tracked by EDCU 1012.

[00136] Customer pending transaction database 1414 may be suitably used to store information related to transactions which have taken place without direct use of the fob 102. More particularly, some transactions, such as preference changes and the like, may be initiated by a fob user through a channel which does not involve use of the fob, for example, through a verbal request over a standard telephone. In such a case, and as detailed further below, this data may be suitably stored in pending transaction database 1414. The transaction data remains in database 1414 until the corresponding fob 102 may be used in conjunction with POS device 110, whereupon fob 102 itself (as well as FODUS 1006) may be updated with this new information.

[00137] Update database 1402 may be suitably used to store other types of transactions (*i.e.*, transactions which may not be classifiable as update, loyalty or pending). For example, update database 1402 may be employed to store file structure updates as detailed below.

[00138] Audit file 1406 may be used to track changes to update database 1404, pending database 1414, database 1402, and, in an illustrated embodiment, loyalty database 1410. In

an alternate embodiment, wherein no separate loyalty database 1410 is used, audit file 1406 may track changes to databases 1404, 1414, and 1402. Audit file 1406 therefore may help to ensure the integrity of data in the respective files.

[00139] Administrative file 1412 may provide suitable database software configured to edit, update, delete, synchronize, and ensure non-corruption of data stored within the various databases that may comprise EDCU 1012 (*i.e.*, databases 1402, 1404, 1410, and 1414).

[00140] Data management module 1416 may provide data management capabilities to facilitate data transfer between fobs 102 and databases 1404, 1414, 1402, and 1410 as well as between these databases and the other systems (*i.e.*, update logic system 1010 and FODUS 1006). Thus, data management module 1416 may act as interface to ensure seamless transfer of data between the various systems.

Network

[00141] The various components, databases, modules, and apparatus described above in connection with the invention are connected via a suitable data communication network. Such a network may consist of various physical connections using a variety of conventional data protocols, for example, the TCP/IP protocol. It will be appreciated that the individual connections between components of the present system may differ. For example, a wireless PCS network may be employed from POS device 110 to secure support client server 1004, while an Internet TCP/IP connection may be employed from FODUS 1006 to the various EDCUs 1012.

[00142] Those skilled in the art will appreciate that a variety of hardware systems are suitable for implementing the present invention. Various modems, routers, CPU's, monitors, back-up systems, power-supplies, and peripherals may be employed to realize the benefits of the present system. In one embodiment, for example, a Compaq Prolinea computer operating in an OS/2 environment using IBM MQ Server software may be used to implement secure support client server 1004, wherein the various POS devices may comprise stand-alone fob kiosks, an EDCU 1012 and FODUS 116 may then be implemented on a Compaq Prolinea

computer operating in a Windows/NT environment running a suitable database software package.

Personalization System

[00143] Referring now to FIG. 18, in an exemplary embodiment, personalization system 116 may suitably comprise a fob management system 1802, a legacy management system 1804, a gather application module 1806, one or more databases 1810, an activation block 1808, a common fob personalization utility 1812 (CCP), a service bureau 1814, a common fob security server 1816, a key management system 1818, and one or more key systems 1820. Personalization system 116 may be in communication with fob 102 via RF ISO 14443 interface 114 for populating fob database 212 with the security keys, for facilitating authentication of the unique RFID reader 104 identifier. In addition, personalization system 116 may populate on database 212 a unique fob 102 identifier for use by RFID reader 104 in determining whether fob 102 may be authorized to access system 100. Personalization system 116 may populate (*e.g.*, inject) the encrypted fob 102 account number into fob database 214 for later providing to authenticated RFID reader 104. Personalization system 116 may additionally populate travel-related information into fob database 212 for later providing to RFID reader 104, third-party travel partners, and/or issuer systems.

[00144] In one exemplary embodiment, personalization system 116 may include any standard computing system as described above. For example, personalization system 116 may include a standard personal computer containing a hardware security module operable using any conventional graphic user interface. Prior to populating the security key information account number, unique identifying information, and travel-related information into fob 102 or RFID reader 104, the hardware security module may authenticate fob 102 and RFID reader 104 to verify that the components are authorized to receive the secure information.

[00145] Key management system 1818 may suitably comprise a database module, CID replace module, key system, and key system. CCP 1812 may suitably communicate with FODUS 1006 (shown in FIG. 10), and legacy management system 1804 may suitably

communicate with account maintenance 142 which may also be configured to communicate with FODUS 1006.

[00146] Fob management system 1802 may suitably receive the fob request 1801 and initiate the gathering of information from various sources. Generally, fob request 1801 may consist of various request information intended to specify a desired group of fob characteristics. Such characteristics may include, for example: a list of desired applications (airline, hotel, rental car, etc.); a designation of whether the fob is new, a renewal, or a replacement; a list of default fob user preferences corresponding to the desired applications; personal information related to the fob user (name, address, etc.); and required security levels.

[00147] Fob management system 1802 may suitably parse the fob request and, for information already stored by the issuer, sends a request to legacy fob management system 1804. For information not available as legacy data, fob management system 1802 may forward the relevant components of fob request 1801 to gather application module 1806. In an exemplary embodiment, fob management system 1802 may choose the optimum fob physical characteristics for a particular fob request 1801. That is, fob management system 1802 may suitably determine the appropriate type of fob chip to be used based on a number of factors, for example, memory requirements and computational complexity of the desired security functions. Similarly, the optimum protocol/sequence controller may be chosen. In an alternate embodiment, the fob transponder, protocol/sequence controller, and the like, may be specified in fob request 1801.

[00148] Legacy management system 1804 may act as a suitable repository of information related to the fob user's past relationship, if any, with the fob issuing organization. For example, a fob user may have a long-standing credit or debit account with issuing organization (based on a standard embossed mag-stripe fob) and this information may be advantageously incorporated into the issued fob.

[00149] Gather application module 1806 may be suitably configured to receive information from fob management system 1802 and legacy management system 1804 and then interface

with the various databases 1810 to gather all remaining application information specified in fob request 1801. In an exemplary embodiment, databases 1810 may correspond to and be associated with the individual partnering enterprises which offer fob applications for use in fob 102 (*e.g.*, networks 112 in FIG. 10). Thus, for example, a fob request 1801 which included a request for a hotel application may trigger gather application 1806 to initiate data communication with the appropriate hotel database 1810. Hotel database 1810 may then return information specifying the correct file structure, access conditions (security), default values, and other data to configure fob 102 with the requested application. Communication with the various databases 1810 may take place through any suitable means, for example, data communication over the Internet, PSTN, and the like, or through other channels, such as simple phone requests.

[00150] Activation block 1808 may be suitably used to provide a means for the fob user to activate the fob once it has been issued. For example, it may be common for credit fobs and the like to be sent to the fob user unactivated, requiring that the fob user call (or otherwise contact) an automated system at the issuer in order to activate the fob. This may typically be accomplished via entry of the fob number and other suitable ID using a touch-tone phone. In this regard, activation block 1808 may be used to facilitate this function for the requested fob (*i.e.*, to specify whether such activation is desired or necessary for a particular fob).

[00151] CCP 1812 may be used to create a correctly formatted fob "object" (*i.e.*, the operating system, file structure and all other available fob data to be downloaded to fob 102) then transfer this information to service bureau 1814 (for creation of the fob) and FODUS 1006 (for recording the fob's state as issued). CCP 1812 may be configured to tailor the format of the fob object to the specific fob issuance system to be used (described below). Thus, gather application system 1806 may deliver a relatively high-level functionality request, and CCP 1812 can create the specific "object" to be used in the implementation.

[00152] Personalization Service Bureau 1814 may comprise suitable hardware and/or software components to complete production of the fobs for issuance to the respective fob

users. In this regard, service bureau 1814 may include a suitable fob "printer" to handle the transfer of information to the fob chip as well as any conventional embossing or mag-stripe writing that may take place.

[00153] Common fob security server 1816 (CCSS) may suitably comprise software and/or hardware components to retrieve cryptographic key information from various enterprise key systems 1820. In an exemplary embodiment, this information may be accessed by service bureau 1814 in order to complete the personalization process. More particularly, it may typically be the case that a fob 102 contains a number of different applications associated with a wide range of enterprise organizations. One skilled in the art will appreciate that the writing, updating, and reading of these files may be advantageously restricted to particular parties in accordance with a set of access condition rules. These access conditions may be suitably implemented using cryptographic keys which are known by the appropriate parties. Thus, service bureau 1814, whose task it is to create and populate the fob file structure, may not, *ab initio*, have access to the keys to perform this function. As mentioned briefly above, known systems have attempted to solve this problem by accumulating key data in a central repository used in the issuance process, thereby creating an unacceptable security risk. Methods in accordance with the present invention, however, may allow for communication between the fob and the individual key systems 1820 as the fob is being issued, thus allowing key information to be securely downloaded to the fob without the intervention of a third party. CCSS 1816 may be suitably used to facilitate this process by receiving information from CCP 1812 regarding the identity of the various applications to be created in the various fobs, then, when prompted by service bureau 1814 (or, alternatively, prior to issuance by service bureau 1814), contacting the appropriate key system 1820 to request a key to be transmitted to service bureau 1814 during personalization.

[00154] Key systems 1820 may comprise suitable database systems capable of storing, generating, and securely transmitting cryptographic keys associated with a particular enterprise. Key management system 1818 may be, in this context, a system comparable to

key systems 1820, but which is "owned" by the party implementing the personalization system. The key-generating function may be distributed between CCSS 1816 and key systems 1820. That is, the keys may be generated in real time at CCSS 1816 (in accordance with algorithms and key information received from the particular enterprises), rather than being generated at key systems 1820.

[00155] It will be appreciated to one skilled in the art that the functional blocks illustrated in FIG. 18 may be implemented using a variety of hardware and/or software components, both off-the-shelf and/or custom-developed. Database-intensive functions performed, for example, by fob management system 1802, may be implemented using any suitable database package, (*e.g.*, Codebase, dBase, or the like).

Personalization Process

[00156] A personalization system as described above in conjunction with FIG. 18 may be suitably used to efficiently issue a large number of fobs with a wide range of functionality levels. This task may involve obtaining and coordinating, in a timely fashion, accurate data for individual fob users across the various partnering enterprises supported by the system. In this regard, it may be the case that certain partnering enterprises desire to limit the dissemination of proprietary data. This data may include, for example, private keys used in connection with fob access conditions as well as file structure and fob user personal data.

[00157] Referring now to FIGS. 18 and 19, an exemplary fob personalization process will now be described. First, the system may receive a fob request (step 1902). As mentioned above, fob management system 1802 may be suitably used to receive the fob request and initiate the gathering of information from various sources. Fob request 1801 may suitably consist of request information intended to specify a desired group of fob characteristics. Such characteristics may include, for example: a list of desired applications (airline, hotel, rental car, etc.); a designation of whether the fob is new, a renewal, or a replacement; a list of default fob user preferences corresponding to the desired applications; personal information related to the fob user (name, address, etc.); and required security levels.

00158] Next, in step 1904, the system may select the fob type and configuration appropriate for the given fob request 1801. This step may be suitably performed by fob management system 1802. Thus, fob management system 1802 may examine a number of factors in light of information received in fob request 1801 (*e.g.*, memory requirements, desired security functions, and the like), then may select an appropriate fob chip from a library of available chips. In the same way, the optimum fob operating system (FOS) may also be selected.

00159] In step 1906, fob user information may be obtained. This step may be suitably performed by gather application module 1806 operating in conjunction with databases 1810 and legacy management system 1804. More particularly, fob user-specific information may be classified in two groups: information known to the personalization system, and information not known by the personalization system. Known information generally may consist of data acquired through a past relationship with the organization hosting the personalization system. In such a case, certain data such as fob user name, preferred billing address, title, company, etc., may most likely already be known, as will certain application data. Such information may be suitably stored in, and may be retrieved from, one or more databases comprising legacy management system 1804. As part of step 1906, the system (specifically, module 1808) may determine whether the fob should require activation. That is, as mentioned briefly above, it may be common to apply a sticker or the like to a fob that notifies the fob user that activation of the fob is required prior to use. Activation typically involves the use of an automated phone system or internet website). The choice of whether a particular fob requires activation may be based on a number of factors, for example, demographics, crime-rate numbers, or mail fraud statistics associated with the fob user's zip-code number.

[00160] For data not included in legacy management system 1804, gather application module 1806 may suitably communicate with databases 1810 to retrieve the information needed to satisfy fob request 1801. This information may typically consist of file structure information (*e.g.*, the DF and EF hierarchy, data types and lengths, and access condition specifications for

the particular enterprise-sponsored application). For example, in the case where fob request 1801 may include a request for an airline application, gather application module 1806 may contact the database corresponding to the enterprise hosting the airline application, then download the relevant file structure information. This process may continue in turn for each new or modified application to be incorporated into the fob.

[00161] In step 1908, a full fob user data set may be created, suitably using CCP 1812. This data set, or "fob object," may ultimately be used by service bureau 1814 to create the physical fob. The form of the fob object may vary. In one embodiment, the fob object may comprise a Binary Large Object ("BLOB"). The fob object may be tailored to the selected fob configuration (*e.g.*, chip type and operating system as specified in step 1904), the content of fob user information data (gathered in step 1906), and the intended fob "printer" (*i.e.*, the apparatus used to create the finished fob within service bureau 1814). This allows the system, in the preceding steps, to specify file structures, data types, and the like, without concerning itself with how this structure will be encoded onto the fob or how the data will be accessed. Up until step 1908, the system need only develop a relatively high-level model of the intended fob data structure; the specifics may be substantially invisible to all but CCP 1812.

[00162] In an alternate embodiment, various details of the fob data object may be determined at a prior point in the system. That is, the functionality of CCP 1812 may be distributed among various components of the system.

[00163] Having created the fob user data set, or fob object, in step 1908, this data may then be sent to FODUS 1006 (step 1910). This ensures that the DSS (particularly FODUS 1006) has a record of the fob state at the time of personalization. This information may then be immediately available to account maintenance system 142.

[00164] The fob object may then be sent to service bureau 1814 and (if required) CCSS 1816 (step 1912). In step 1914, the relevant keys may be acquired to allow service bureau 1814 to create the finished fob. As mentioned above, step 1914 may be suitably performed by CCSS

1816 concurrently or serially with the issuance process. In one embodiment, as each individual fob may be being created using an issuance system suitably located at service bureau 1814, service bureau 1814 interrogates CCSS 1816 for the appropriate cryptographic keys. These keys have either been retrieved from key systems 1820 and 1818 earlier (*i.e.*, after step 1912), or may be retrieved in real-time in response to the request from service bureau 1814. Alternatively, the keys may be retrieved by CCSS 1816 and transmitted to CCP 1812 prior to transmission of the fob object to service bureau 1814. In either case, the key or keys may then be retrieved for inclusion in the fob object created in step 1908.

[00165] In step 1916, the actual fob may be issued. Service bureau 1814 may suitably download the fob object into the correct fob hardware using the correct cryptographic keys. The initialized fob may then be packaged and distributed to the appropriate fob user in accordance with conventional methods.

Synchronization Process

[00166] A dynamic synchronization system as described above in various embodiments may be used to track the "state" of the consumer's fob. The state of the fob may be suitably characterized by the structure of applications used in the fob and the various pieces of data that are stored within these applications.

[00167] The manner in which applications and data are managed within a fob can vary. For example, data files and directories may be stored in a "tree" structure in fob 102. That is, the fob file structure suitably resembles the well-known MS-DOS (Microsoft Disk Operating System) file structure wherein files are logically organized within a hierarchy of directories. Specifically, three types of files are defined in ISO 7816-4: dedicated files (DF), elementary files (EF), and a master file (MF). The master file may be analogous to the MS-DOS "root" directory, and contains all other files and directories. Dedicated files may actually be directories or "folders" for holding other DFs or EFs. Thus, the MF may contain an arbitrary number of DFs, and these DFs may or may not contain other DFs. Elementary files may be used to store user data, and may exist within a dedicated file, or within the master file.

Higher level DFs (*i.e.*, DFs which house particular applications) are often referred to as application dedicated files (ADFs). The scope of the present invention is not, however, limited to this type of multi-function fob. Other implementations, for example, Multos or Java-based fobs, may also be suitable within the context of the instant invention.

[00168] A number of synchronization issues may arise in the multi-function fob context; indeed, three paradigmatic cases reoccur with some frequency, and relate to: 1) update transactions, 2) pending transactions, and 3) file structure changes. Each of these cases will now be described in turn with respect to the present invention.

Example 1: Update Transactions

[00169] It may be quite common for a fob user to make a local change to fob 102 which may not be immediately reflected in all the databases which could advantageously make use of this information. For example, suppose that upon initialization (*i.e.*, when the fob was originally issued via personalization system 116) the fob user's fob 102 was configured to reflect a general preference for smoking (*e.g.*, one file contains a Boolean field keyed to smoking/non-smoking), but the fob user now wishes to change this general preference file to reflect a non-smoking preference.

[00170] In this case, referring now to FIGS. 10 and 17, and with respect to an exemplary embodiment, the fob user suitably may use fob 102 to communicate with a conveniently located POS device 110 via RFID reader 104, whereupon authentication of the fob and/or fob-reader may take place (step 1702). In an exemplary embodiment, authentication may take place in accordance with relevant sections of the ISO 7816 standard.

[00171] Next, the fob user may use a suitable user interface (supplied by POS device 110 working in conjunction with server 1004) in order to perform a transaction (*i.e.*, to request a change to the preferences file) (step 1704). This change may typically be reflected at the fob 102 immediately. That is, POS device 110 and/or server 1004 may include the functionality to access and update the appropriate files within fob 102.

[00172] Communication router 1106 in server 1004 may then routes the transaction to the appropriate party (*i.e.*, an EDSI 1008 or an EDCU 1012) corresponding to branches 1707 and 1705 respectively. That is, depending on the system configuration, the file to be changed may be associated with a particular enterprise or, alternatively, may be associated with the organization hosting the DSS. These two cases are described in turn.

[00173] Following branch 1707 in FIG. 17, the change data may be sent to and stored in the appropriate EDSI 1008 (step 1708). Update logic system 1010 may then transfer this change request to the appropriate EDCU 1012 (*i.e.*, the EDCU 1012 corresponding to the particular EDSI) (step 1710). This information may be suitably stored in the corresponding update database 1404. The information may be also distributed to other EDSIs. In the instant example, update logic system 1010 may identify those systems that may benefit from knowing the fob user's smoking status. Such systems may include, for example, various hotels, rental car agencies, and the like.

[00174] Alternatively, following branch 1705 in FIG. 17, the data may first be stored at the appropriate EDCU (step 1712), then distributed to other EDUCs 1012 and EDSIs 1008 as described above.

[00175] The fob data change may then be transferred to FODUS 1006. Specifically, the various fields and files associated with the fob 102 may be updated to reflect the change stored in update database 1404. Thus, the information within FODUS 1006 may conform to that contained within fob 102 and the various EDCUs 1012 and EDSIs 1008. After this transfer, the corresponding change data in update database 1404 may be cleared (step 1718).

Example 2: Pending Transaction

[00176] The fob user may make a change or perform a transaction through a channel that does not directly involve fob 102, thus creating an inconsistency between the data in fob 102 and the data in various databases throughout the DSS. Such a case may arise, for example, when the fob user calls a hotel to make a reservation (rather than performing the transaction on line

using fob 102) and makes an oral request to change his preferences from smoking to non-smoking.

[00177] Referring now to FIGS. 10 and 16, in this case, with respect to an exemplary embodiment of the present invention, the fob user first may contact an enterprise through a means that does not include fob 102 (*i.e.*, a "fob not present" transaction) (step 1602). Using an appropriate interface (voice, keypad, etc.), a change or transaction may be selected (step 1604). This change may then be stored locally within a particular network 112 and/or may be stored within an EDSI 1008 (step 1606).

[00178] Next, in step 1608, update logic system 1010 may route this information to the corresponding EDCU 1012, where it resides in pending database 1414. At this point, fob 102 itself may be oblivious to the change. As a result, if the fob user were to initiate a fob-present transaction, the corresponding enterprise may likely look first to the data structure in fob 102 for preferences, and as just stated, may most likely arrive at the wrong conclusion (*e.g.*, a smoking room may be assigned notwithstanding the fob user's expressed preference).

[00179] In order to remedy this situation, the present invention provides, in steps 1610 and 1612, a method by which the fob may be updated upon its next use. That is, after fob 102 may be used to communication with POS device 110 via RFID reader 104 and may be suitably authenticated (step 1610), the system interrogates pending database 1414 to determine whether any changes have been made. If so, the appropriate information may be downloaded to fob 102 (step 1612).

[00180] After the above information transfer is successfully completed, the change data may be transferred to FODUS 1006 (step 1614), where it may be stored within fob object database 212. Finally, the respective information within pending database 1414 may be cleared (step 1616).

Example 3: File Structure/Application Change

[00181] In addition to the data-related modifications detailed above, changes to the structure of data stored in fob 102 may also be desirable in certain contexts. That is, during the life of

a fob, it may be likely that the fob issuer, a partnering enterprise, or the fob user himself may desire to extend the fob's functionality by augmenting the suite of applications housed within the fob. For example, a fob user who may use a fob for rental car and airline reservations may also wish to use the fob for acquiring and paying for hotel reservations. In such a case, the appropriate hotel partner may process the fob user's request and arrange for addition of a hotel application to be added to the fob file structure. In another example, the fob issuer may authorize the addition of a new application on its own, for example, a credit and/or debit application. Conversely, it may also be appropriate in some instances to remove applications from the fob.

[00182] In an exemplary embodiment, the types of file structure changes described above may be handled in a manner analogous to the procedure set forth in FIG. 16, depending, to some extent, upon which party originates the file structure change. That is, as in step 1612, the appropriate file structure change information may be stored in EDCU 1012 (for example, in database 1402), and then transferred to fob 102 when the fob is used in conjunction with an on-line transaction (steps 1610 and 1612). After the file structure on fob 102 is augmented or otherwise modified, FODUS 1006 (specifically, database 1016) may be similarly modified to reflect the change. The change information may then be cleared from database 1402 (step 1616).

[00183] Although the invention has been described herein in conjunction with the appended drawings, those skilled in the art will appreciate that the scope of the invention is not so limited. Modifications in the selection, design, and arrangement of the various components and steps discussed herein may be made without departing from the scope of the invention as set forth in the appended claims. For a detailed explanation of dynamic synchronization and personalization for a smartcard, see U.S. Pat. No. 6,199,762, dated March 13, 2001, titled "METHODS AND APPARATUS FOR DYNAMIC SMARTCARD SYNCHRONIZATION AND PERSONALIZATION," incorporated herein by reference.

[00184] Benefits, other advantages, and solutions to problems have been described herein with regard to specific embodiments. However, the benefits, advantages, solutions to problems, and any element(s) that may cause any benefit, advantage, or solution to occur or become more pronounced are not to be construed as critical, required, or essential features or elements of any or all the claims or the invention. As used herein, the terms "comprises," "comprising," or any other variation thereof, are intended to cover a non-exclusive inclusion, such that a process, method, article, or apparatus that comprises a list of elements does not include only those elements but may include other elements not expressly listed or inherent to such process, method, article, or apparatus. Further, no element described herein is required for the practice of the invention unless expressly described as "essential" or "critical."

What is claimed:

1. A system for facilitating synchronizing transponder information associated with a transponder, said system comprising:

a first enterprise data collection unit associated with a first enterprise, said enterprise data collection unit configured to store update transactions and pending transactions associated with said transponder and said first enterprise;

a second enterprise data collection unit associated with a second enterprise, said second enterprise data collection unit configured to store update transactions and pending transactions associated with said transponder and said second enterprise;

at least one point-of-sale device configured with a transponder-reader to interface with said transponder and said first and second enterprise data collection units;

a fob object database system coupled to said first and second enterprise data collection units and configured to store said transponder information in accordance with said update transactions and said pending transactions, wherein said transponder information may include a fob object having at least one application; and

an update logic system configured to route said transponder information from said first and second enterprise data collection units to at least one of said point-of-sale device in order to effect synchronization of said transponder information associated with said fob and said fob object database system.

2. A system according to claim 1, further comprising an update logic system coupled to at least one enterprise data synchronization interface, said update logic system configured to securely route transponder information between said enterprise data synchronization interface and said enterprise data collection units, said enterprise data synchronization interface coupled to an enterprise network configured to communicate with said point-of-sale device.

3. The system according to claim 2, further comprising a secure support client server configured to communicate with said point-of-sale device, said secure support client server further configured to adaptively provide communication functionality in accordance with the communication functionality available at said point-of-sale device.

4. The system of claim 1, further including a personalization system comprising:

a security server;

at least one key system associated with said at least one application, said key system configured to communicate with said security server and to supply a key in response to a request from said security server;

a personalization utility configured to receive said fob object and to communicate with said security server;

said personalization utility further configured to add said key to said fob object;

a transponder management system, said transponder management system configured to accept a transponder request and communicate said transponder request to said personalization utility; and

a gather application module configured to communicate with said transponder management system and gather application information from a first database and a second database in accordance with said transponder request, wherein said first database is associated with said first enterprise, and said second database is associated with said second enterprise.

5. A personalization system comprising:

a security server;

at least one key system associated with said at least one application, said key system configured to communicate with said security server and to supply a key in response to a request from said security server;

a personalization utility configured to receive a fob object and to communicate with said security server;

said personalization utility further configured to add said key to said fob object;

a transponder management system, said transponder management system configured to accept a transponder request and communicate said transponder request to said personalization utility;

a first enterprise data collection unit associated with a first enterprise, said enterprise data collection unit configured to store update transactions and pending transactions associated with said transponder and said first enterprise;

a second enterprise data collection unit associated with a second enterprise, said second enterprise data collection unit configured to store update transactions and pending transactions associated with said transponder and said second enterprise; and

a gather application module configured to communicate with said transponder management system and gather application information from a first database and a second database in accordance with said transponder request, wherein said first database is associated with said first enterprise, and said second database is associated with said second enterprise.

6. The system of claim 5 wherein said transponder management system is further configured to parse said transponder request in order to choose optimum transponder characteristics.

7. The system of claim 5 wherein said personalization utility is further configured to facilitate formatting said fob object.

8. The system of claim 5 further comprising an activation block configured to facilitate activation of a transponder.

9. A method for personalization comprising the followi

communicating with a security server to facilitate supplying a key in response to a request from said security server;

receiving a fob object at a personalization utility configured to communicate with said security server;

using said personalization utility to facilitate adding said key to said fob object;

accepting a transponder request at a transponder management system to facilitate communicating said transponder request to said personalization utility;

storing update transactions and pending transactions at a first enterprise data collection unit associated with a transponder and a first enterprise;

storing update transactions and pending transactions at a second enterprise data collection unit associated with a transponder and a second enterprise; and

gathering application information from a first database and a second database in accordance with said transponder request, wherein said first database is associated with said first enterprise, and said second database is associated with said second enterprise, and wherein said step of gathering comprises using a gather application module configured to communicate with said transponder management system.

10. The method of claim 9 wherein said step of gathering application information from a first database and a second database in accordance with said transponder request further comprises creating at least one of a file structure, data set and data type.

11. The method of claim 9 further comprising the step of issuing a transponder corresponding to said transponder request.

12. A method for facilitating synchronizing transponder information associated with a transponder, said method comprising the following steps:

using a first enterprise data collection unit associated with a first enterprise to facilitate storing update transactions and pending transactions associated with said transponder and said first enterprise;

using a second enterprise data collection unit associated with a second enterprise to facilitate storing update transactions and pending transactions associated with said transponder and said second enterprise;

interfacing with said transponder and said first and second enterprise data collection units through at least one point-of-sale device configured with a transponder-reader;

storing said transponder information in accordance with said update transactions and said pending transactions at a fob object database system coupled to said first and second enterprise data collection units, wherein storing said transponder information may include storing a fob object having at least one application; and

using an update logic system to facilitate routing said transponder information from said first and second enterprise data collection units to at least one of said point-of-sale device in order to effect synchronization of said transponder information associated with said fob and said fob object database system.

13. The method of claim 12, further comprising the step of using an update logic system coupled to at least one enterprise data synchronization interface to facilitate securely routing transponder information between said enterprise data synchronization interface and said enterprise data collection units, said enterprise data synchronization interface coupled to an enterprise network configured to communicate with said point-of-sale device.

14. The method of claim 12, wherein said step of communicating with said point-of-sale device using a secure support client server, wherein said step of using said secure support client server further comprises adaptively providing communication functionality in accordance with the communication functionality available at said point-of-sale device.

15. The method of claim 12, further comprising the step of facilitating personalization, wherein said step comprises:

communicating with a security server to facilitate supplying a key in response to a request from said security server;

receiving a fob object at a personalization utility configured to communicate with said security server;

using said personalization utility to facilitate adding said key to said fob object;

accepting a transponder request at a transponder management system to facilitate communicating said transponder request to said personalization utility;

storing update transactions and pending transactions at a first enterprise data collection unit associated with a transponder and a first enterprise;

storing update transactions and pending transactions at a second enterprise data collection unit associated with a transponder and a second enterprise; and

gathering application information from a first database and a second database in accordance with said transponder request, wherein said first database is associated with said first enterprise, and said second database is associated with said second enterprise, and wherein said step of gathering comprises using a gather application module configured to communicate with said transponder management system.

16. The method of claim 12, wherein step of routing said transponder information from said first and second enterprise data collection units comprises routing said transponder information in track 1/track 2 International Standards Setting Organization format.