



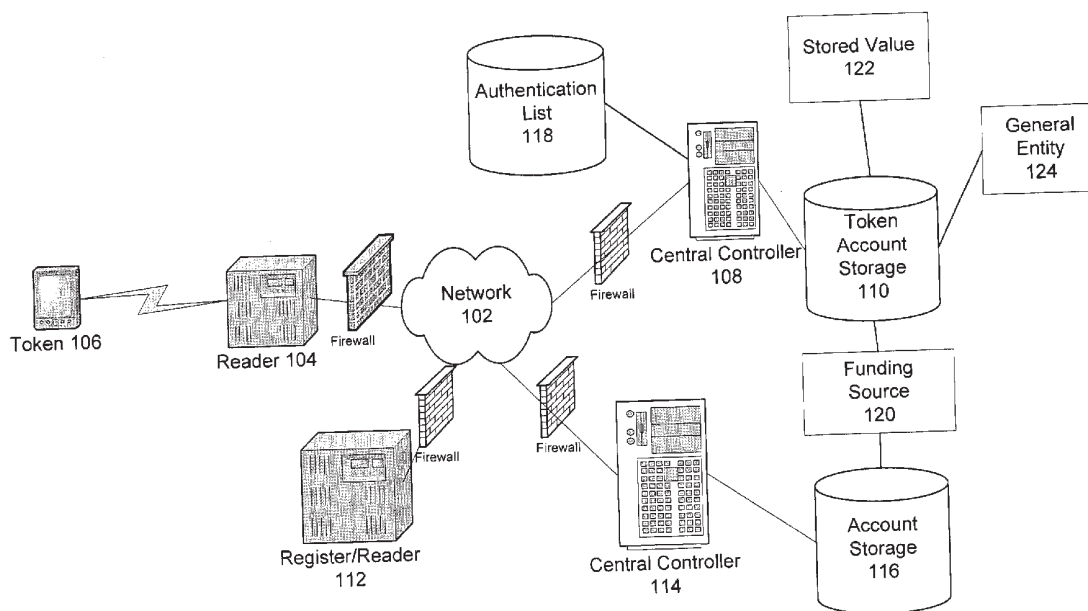
US 20030187787A1

(19) **United States**(12) **Patent Application Publication**
Freund(10) **Pub. No.: US 2003/0187787 A1**(43) **Pub. Date: Oct. 2, 2003**(54) **SYSTEM AND PROCESS FOR PERFORMING
PURCHASE TRANSACTIONS USING
TOKENS****Publication Classification**(51) **Int. Cl.⁷ G06F 17/60**(76) **Inventor: Peter C. Freund, New York, NY (US)**(52) **U.S. Cl. 705/39; 705/40**

Correspondence Address:

HUNTON & WILLIAMS**INTELLECTUAL PROPERTY DEPARTMENT****1900 K STREET, N.W.****SUITE 1200****WASHINGTON, DC 20006-1109 (US)**(57) **ABSTRACT**(21) **Appl. No.: 10/401,749**(22) **Filed: Mar. 31, 2003****Related U.S. Application Data**(60) **Provisional application No. 60/368,155, filed on Mar.
29, 2002.**

The invention relates to a method and process by which an existing and large network of devices can be used by consumers to authenticate themselves, and permits each consumer to apply any of the various payments mechanisms available to him. The existing broadly distributed network is active and passive radio frequency identification ("RFID") devices held by consumers. Various types of accounts are linked to devices and allow users to perform various purchase transactions, as well as nonfinancial transactions.



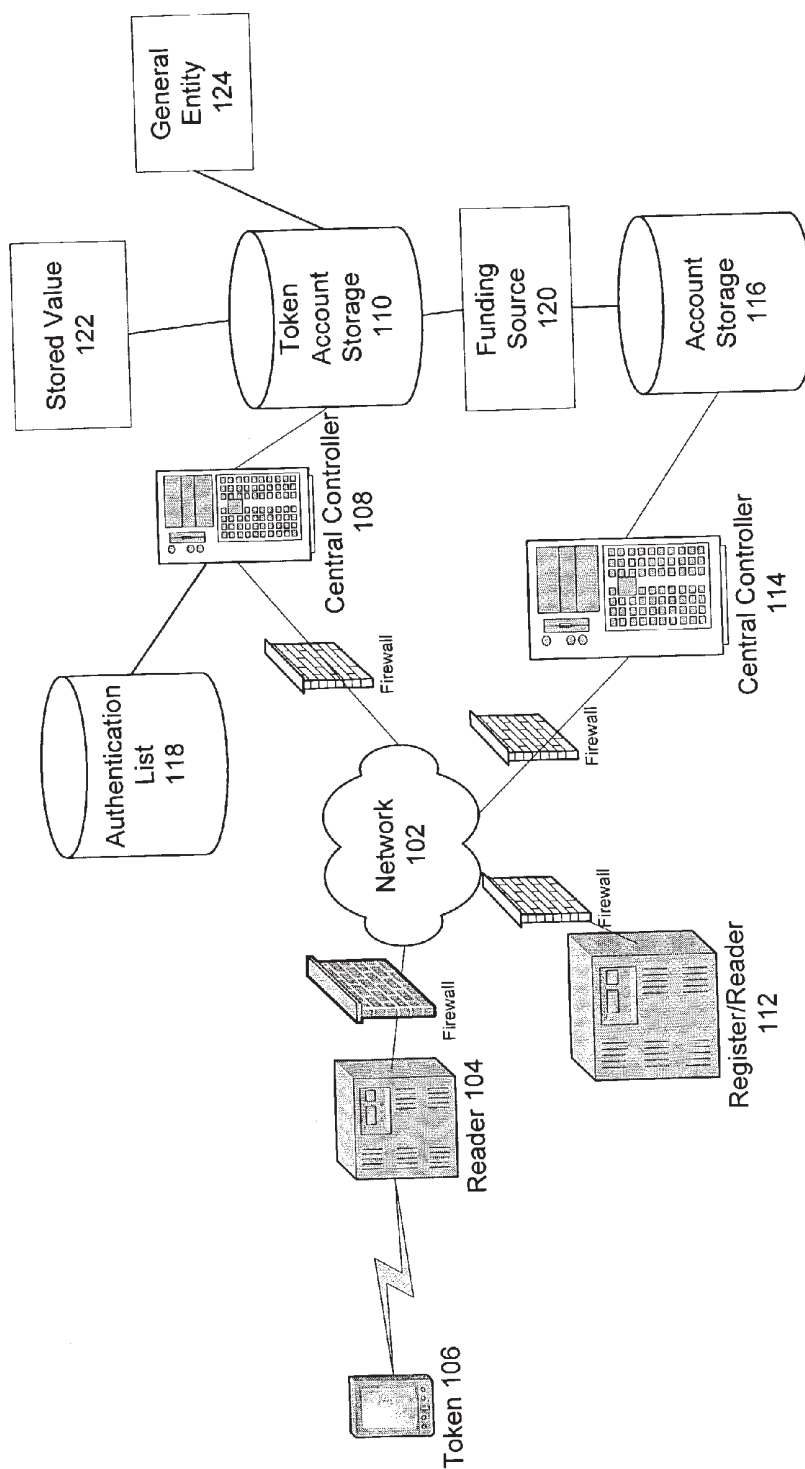


Fig. 1

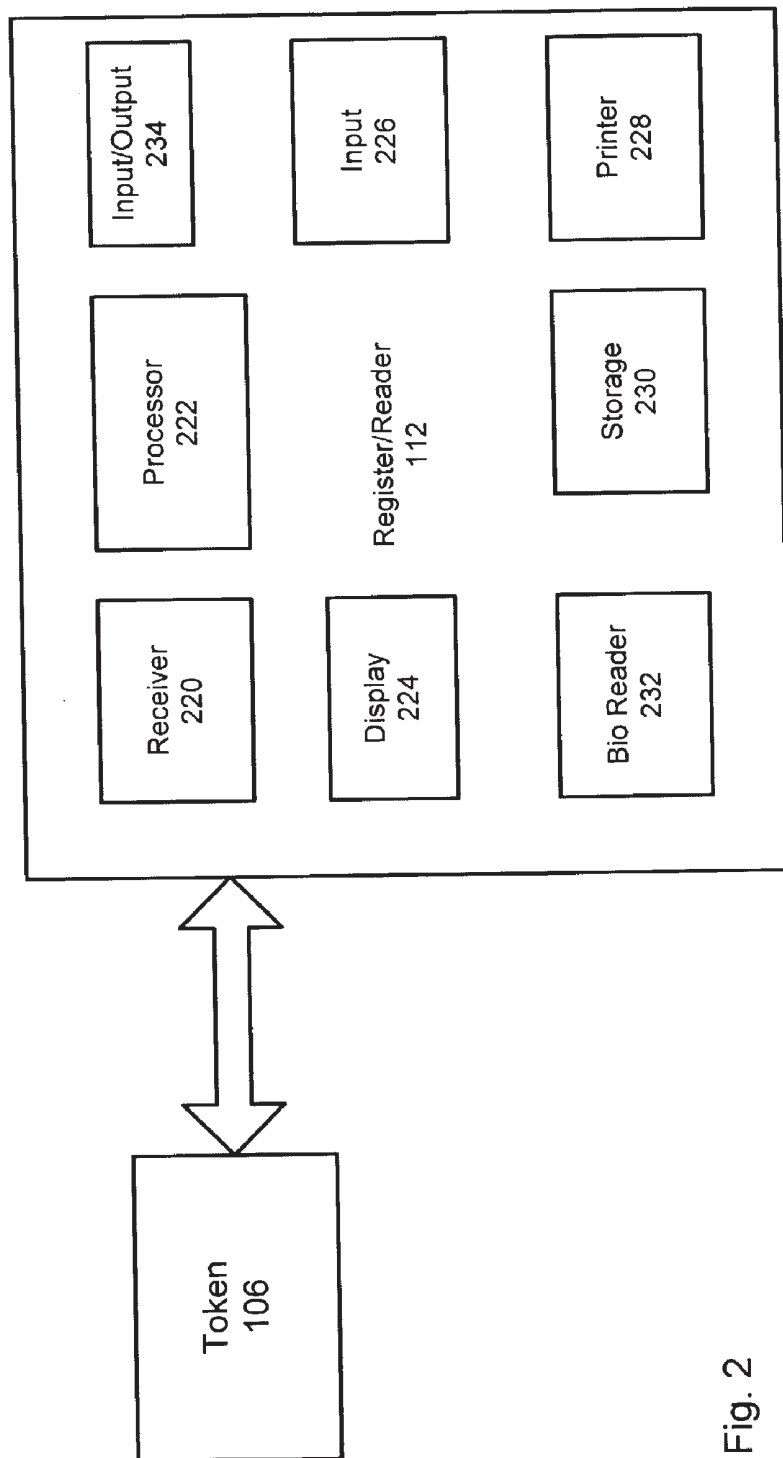


Fig. 2

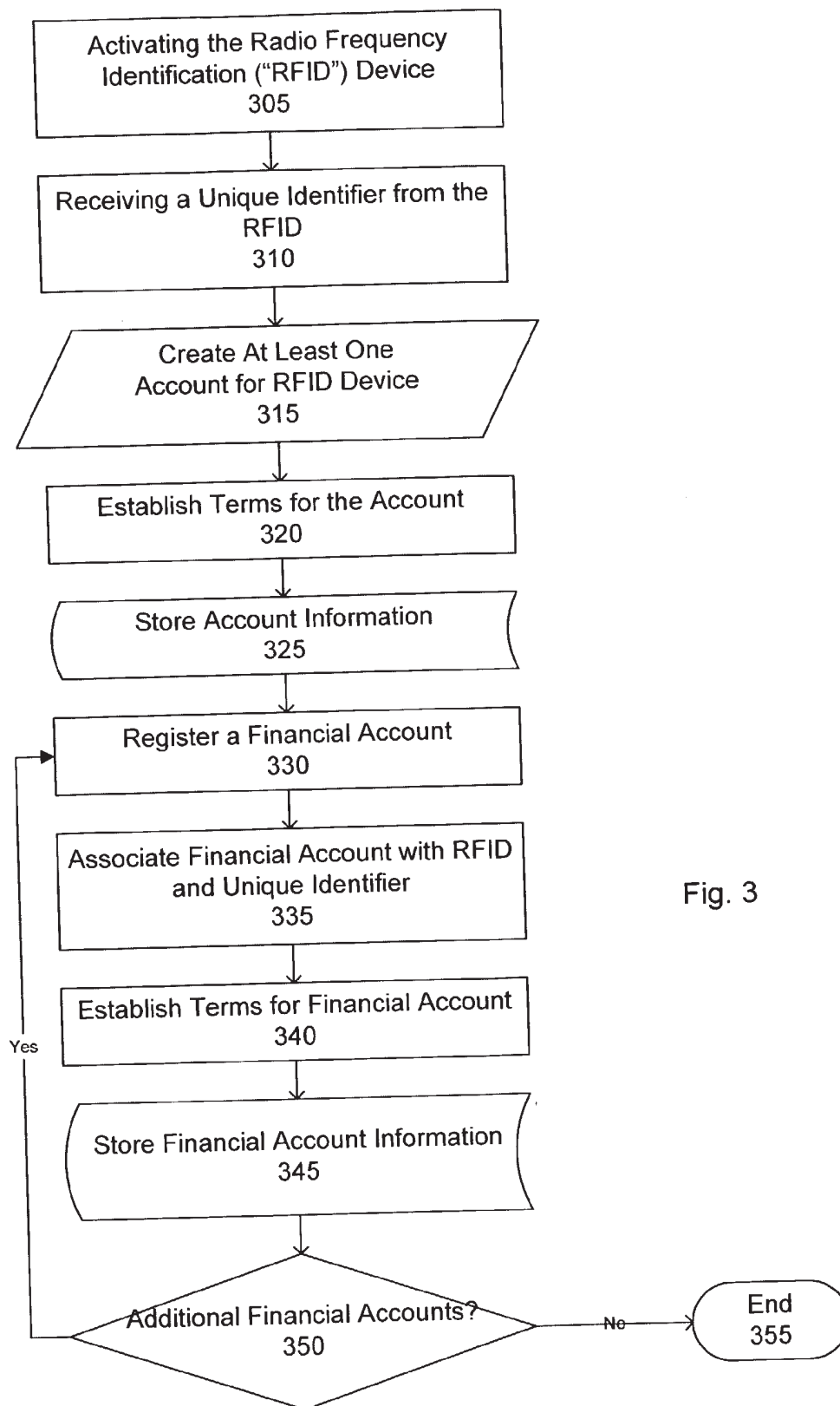


Fig. 3

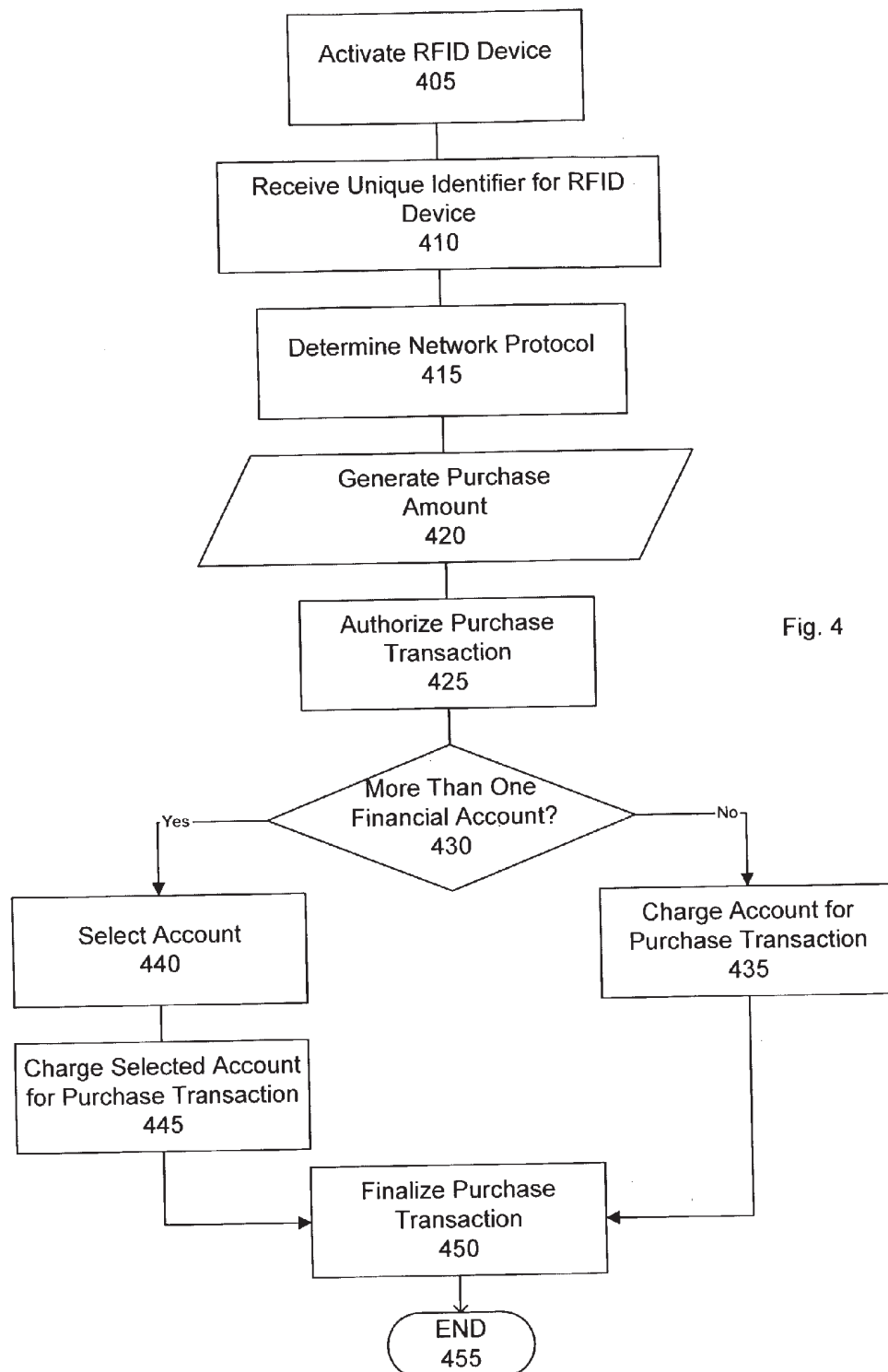


Fig. 4

SYSTEM AND PROCESS FOR PERFORMING PURCHASE TRANSACTIONS USING TOKENS

PRIORITY

[0001] The present application claims priority to Provisional Application Serial No. 60/368,155, filed on Mar. 29, 2002.

FIELD OF THE INVENTION

[0002] The present invention relates generally to authentication tokens used for performing purchase transactions and other functionality, and more specifically to radio frequency identification devices for performing purchase transactions with an automobile as a trusted entity.

BACKGROUND OF THE INVENTION

[0003] Technologically new payments mechanisms have often been frustrated by the famous 'chicken or the egg' conundrum. Until there are lots of consumers with the new devices, merchants are reluctant to pay the cost of installing new readers for the technology. Similarly, consumers are reluctant to carry new devices until there are enough merchants to accept them. Despite increasing fraud associated with criminals 'stripping' the information from magnetic-stripe cards, the card associations have failed to deploy more secure alternatives. Smartcards are just one example of the devices that have failed to gain traction. The invention described here addresses this conundrum.

[0004] RFID technology is very broadly used today. RFID devices are currently used to identify: cattle; packages; owners of vehicles and for payments (e.g. the 5 MM active Exxon Mobil SpeedPass users). The technology is available in two forms, active and passive RFID devices.

[0005] E-Z Pass is an example of an active RFID device. In order to permit cars to be recognized at speeds up to 200 MPH, such active RFID devices have a battery and in response to a signal from readers, transmit a signal that can be recognized from a distance of 40 meters from the reader. At such distances, it is important that only the intended vehicle is charged for the toll. As a consequence, a lot of technology is focused on tracking a particular vehicle within a specific lane of traffic.

[0006] One large implementation of RFID technology is connected to passive devices. Passive RFID devices have no battery. These devices contain chips and an antenna. When the passive RFID device is in proximity of a reader, usually within inches but can be feet away, the chip is activated by an RF signal sent by the reader. The reader's broadcast RF signal is captured by the passive device's antenna and generates sufficient electrical energy to activate the chip. The passive RFID chip is hardwired to respond in a particular way, to be recognized by the reader.

[0007] Payments using RFID devices are beginning to emerge, though there are two impediments: merchants have balked at the \$5,000-15,000 cost of installing RFID readers, because there are few RFID enabled consumers; and, issuers are reluctant to distribute tokens (at a cost of \$8 each) unless there are enough merchants to generate sizeable payments.

[0008] The leading RFID payments providers include EZPass, Speedpass, 2Scoop and Freedompay. The primary

goals for these entities are: to broaden as quickly as possible the number of merchants that accept RFID tokens; and to permit consumers freedom to choose multiple payment alternatives with a single token.

[0009] Many of the Exxon Mobil gas stations are Speedpass enabled. In addition, a number of McDonalds restaurants in the Chicago area are now using Speedpass payments, and one grocery store chain began piloting Speedpass in late 2002. However, even with all this new development, RFID payments are still rare.

[0010] Other drawbacks may also be present.

SUMMARY OF THE INVENTION

[0011] Accordingly, one aspect of the invention is to address one or more of the drawbacks set forth above.

[0012] Automobiles (or active communications devices) could be certified as trustworthy in applying and enforcing policies and procedures that will provide an environment for secure payments and other transactions. Current automobile design, including the use of electronic engine controllers (each of which have their own unique electronic identity) could be adjusted to include such functionality, and permit each particular car to include with each payment assurance proffered to counterparties its cryptographic certification electronically. The certification, could be standardized so the counterparties could clearly understand the level of trust applicable to a particular car. The car could also act as a conduit, trusted because of its certification to pass the credentials of the RFID device through to counter parties.

[0013] According to an exemplary embodiment of the invention, a system for performing at least one payment transaction includes a token having a unique identifier associated with a user or key of a particular automobile, where the automobile is held out as an entity trusted by merchants and the token interacts with a reader in the automobile to perform the at least one payment transaction and at least one account associated with the token, where the at least one account makes payments as directed by interaction of the token and the automobile reader.

[0014] According to a further exemplary embodiment of the invention, a system for registering a token includes means for receiving a unique identifier from the token, where the token and the unique identifier are associated with a user or key of a particular automobile, the automobile is held out as an entity trusted by a merchant and the token interacts with a reader to perform the at least one payment transaction, means for creating at least one account associated with the token, where the account includes account information and makes payments as directed by interaction of the token and the reader, means for receiving terms for the at least one account and means for storing the account information and the terms of the at least one account.

[0015] By way of another exemplary embodiment, a process for registering a token is provided, where the process includes receiving a unique identifier from the token, where the token and the unique identifier are associated with a user or key of a particular automobile, the automobile is held out as an entity trusted by a merchant and the token interacts with a reader to perform the at least one payment transaction, creating at least one account associated with the token, where the account includes account information and makes

payments as directed by interaction of the token and the reader, receiving terms for the at least one account and storing the account information and the terms of the at least one account.

[0016] Another embodiment of the invention provides a computer readable medium having code for causing a processor to register a token. The medium includes code for receiving a unique identifier from the token, where the token and the unique identifier are associated with a user or key of a particular automobile, the automobile is held out as an entity trusted by a merchant and the token interacts with a reader to perform the at least one payment transaction, code for creating at least one account associated with the token, where the account includes account information and makes payments as directed by interaction of the token and the reader, code for receiving terms for the at least one account and code for storing the account information and the terms of the at least one account.

BRIEF DESCRIPTION OF THE DRAWINGS

[0017] FIG. 1 illustrates a system for performing purchase transactions with a token according to an embodiment of the invention.

[0018] FIG. 2 illustrates a system for a reader and register according to an embodiment of the invention.

[0019] FIG. 3 is a flow chart illustrating a process for performing token and account registration according to an embodiment of the invention.

[0020] FIG. 4 is a flow chart illustrating a process for performing token and account registration according to an embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0021] A system and process for using a token for performing purchase transactions is described. The system and process makes use of existing tokens distributed for other purposes or for purposes of payment, as well as newly distributed tokens, such as radio frequency identification devices, to perform purchase transactions. One technical effect of the invention is to provide a system and process for performing purchase transactions using, among other items, a radio frequency identification device, as set forth in the Brief Description of the Invention, above and as more fully described here in the Detailed Description of the Invention. Various aspects and components of this system and process are described below. While the present invention is described in terms of tokens, and radio frequency identification devices in particular, it is recognized that other types of tokens may also be used.

[0022] The invention relates to a method and process by which an existing and large network of devices, as well as newly distributed devices, can be used by consumers to authenticate themselves, and permits each consumer to apply any of the various payments mechanisms available to him. The existing broadly distributed network is active and passive radio frequency identification ("RFID") devices held by consumers.

[0023] FIG. 1 illustrates a system for performing purchase transactions with a token according to an embodiment of the

invention. System **100** includes a network **102**, such as the internet, or other type of network. Reader **104** reads token **106**. In the example illustrated in FIG. 1, token **104** is an RFID device and reader **106** is equipped to read the RFID. However, it is recognized that other tokens may also be used. Further, while only one of each item is described for the convenience of explanation, it is understood that multiple devices may be used within the system **100**.

[0024] System **100** also includes a central controller **108** and a token account storage device **110**. Central controller **108** connects with network **102** and interfaces between network **102** and token account storage device **110**. Token account storage device **110**, which may include one or more devices, stores information about the accounts associated with token **106**. Each token **106** has a unique identifier associated with the token. Further, one or more accounts are associated with the token **106**. Accounts may include a specific account associated solely with the token **106**. This account may store funds, such as a stored value card, or may have a line of credit that is paid off periodically, such as a credit card. Further, other accounts may also be associated with the token **106**, such as debit accounts, credit card accounts, and other types of financial accounts. Token account storage device **110** may communicate with funding sources **120** to perform the purchase transaction. According to an embodiment of the invention, payment may be made directly by a transfer of funds from the user of the token to the merchant operating the reader, such as by a transfer of funds from a financial account of the user to the financial account of the merchant. Thus, a direct payment may be made with relatively little time delay.

[0025] According to an embodiment of the invention, indirect payments may be made, with an entity trusted by a merchant serving to act as an intermediary guaranteeing payment. Payments are not made immediately, but the intermediary guarantees the merchant will be paid, thereby facilitating the performance of the purchase transaction. By way of example, an automobile manufacturer may provide a service (e.g., On Star provided by General Motors) to purchasers of the automobile that provides road-side assistance, navigation assistance, and the like. The service may also provide a guarantee of payment to a merchant on behalf of the automobile owner. The merchant then may move forward with the purchase transaction, while the actual payment is made at a later time.

[0026] According to an embodiment of the invention, funding sources **120** may include any source of funds, such as a bank, lender, company, or any other source of funding, such as institutions associated with financial accounts. Further, stored value device **122** may contain funds for performing purchase transactions. For example, funds from a financial account may be transferred into stored value device **122** and then accessed to perform a purchase transaction. According to an embodiment of the invention, funds from stored value device **122** may be used to perform certain types of purchase transactions (e.g., certain merchants, transactions below a certain monetary threshold, etc.). General entity **124** is accessed by token account storage **110** to enable other transactions to be performed, such as accessing medical records, and transferring information.

[0027] An example of passive RFID technology is the anti-theft technology used by auto companies. Historically,

car keys depended on simple mechanical locking systems. Cars have increased in value, and now these simple mechanical systems provide inadequate security. Today, most cars use both a mechanical locking system and an RFID authentication system. In addition to the standard mechanical lock, car companies have provided a much more rigorous electronic protection mechanism. Keys contain RFID chips, and built into the ignition switch is an RFID reader. Even if the mechanical key is replicated, unless the RFID reader validates the key, the car will not start. The engine controller, an electronic chip buried deep within the engine itself, must recognize the RFID device or the engine will not start.

[0028] Many passive RFID tokens for the automotive industry use automotive anti-theft 'cryptographic challenge/response protocol.' This protocol used by auto companies does not rely on a singular ID number hardwired into every RFID device. However, that singular identity number is always accessible using a standards based (QS2000) protocol. It is that identity number that is used for all Speedpass and 2Scoot devices. The RFID identity number is unique and can be used to access any payments system available to the owner of the token. An RFID device may use a standard protocol to provide a transport mechanism for information, such as the frequency of the RFID device, etc. According to an embodiment of the invention, security protocol may also be proprietary to a receiver. However, non secret information may be available to all, such as that every RFID device has unique number and that the unique number is necessary for access.

[0029] Authentication list 118 determines if reader 104 and/or token 106 is authentic and permitted to perform transactions. Authentication list may be used as security to reduce the chances of fraud. According to an embodiment of the invention, token 106 may include information about the address (e.g., internet address) of central controller 108. Reader 104 may then access central controller 108 to perform the purchase transaction. Authentication list 118 may be accessed to ensure that token 106 is allowed to perform a transaction. For example, authentication list 118 may contain a list of tokens 106 that are in good standing, or that are delinquent. While FIG. 1 illustrates authentication list 118 in communication with central controller 108, it is understood that authentication list 118 may be in communication with or resident on reader 104 and/or register/reader 112. Authentication list 118 may also ensure that reader 104 is allowed to access central controller 108. According to an embodiment of the invention, authentication list 118 may also include a list of authorized readers and register/readers that are permitted to access central controller 108.

[0030] System 100 of FIG. 1 also includes a register/reader 112. It is understood that while the reader 104, and the register/reader 112 are included in system 100, other types of readers and devices for token 106 to interact with network 102 may also be used. Further, various functionalities may be provided by register/reader 112 as necessary to implement one or more aspects of the present invention. Register/reader 112, described in greater detail in FIG. 2 below, enables a user to register a token, register a financial account to be associated with the token, provide terms for purchase transactions and other information.

[0031] FIG. 2 illustrates token 106 in communication with reader/register 112. According to an embodiment of the invention, reader/register includes a receiver 220, processor 222, display 224, input 226, printer 228, storage 230, bioinformatics reader 232 and input/output 234. According to the embodiment illustrated in FIG. 2, token 106 is an RFID device. Transceiver 220 receives signals from token 106 and transmits signals to token 106. The signals are converted and sent to processor 222 for appropriate processing. Information from the processing may be displayed at display 224. Display 224 may include a RGB monitor or other manner of displaying information. For example, display 224 may display the amount of the purchase transaction, and, where token 106 with a plurality of accounts associated to it, a selection of which account to perform the purchase transaction. Other functionalities, such as a security and encryption, customer loyalty programs, and approval lists, may also be available in register/reader 112.

[0032] Input 226 enables a user to interact with register/reader 112. Input 226 may include a keyboard, touch-screen, mouse, number pad or other manner of inputting information. For example, where token 106 has a plurality of accounts associated with it, display 224 may display options for the financial accounts to perform the purchase transaction. The user can select the appropriate financial account using input 226. At the conclusion of the purchase transaction, a receipt may be printed by printer 228.

[0033] Information from the purchase transaction is stored in storage 230. Information may then be transmitted through input/output module 234 to the network. For example, information may be stored in storage 230 for a set period of time, and then communicated to purchase transaction account storage 116 (e.g., hourly, daily, weekly, monthly, etc.).

[0034] In addition, bio-metrics module 232 provides biometric information about the user of the token 106. Biometric module 232 may be a retina scan, a finger print reader or other manner of providing bio-metric information. According to an embodiment of the invention, for some information and transactions, it may be desirable for the user of token 106 to confirm his or her identity. This may be confirmed by providing bio-metric information, by entering a personal identification number ("PIN") through input 226, or through other manners of confirmation.

[0035] For example, at a bank, office or store, a register/reader station for RFID tokens may have side-by-side a normal magnetic-stripe reader and a RFID reader. The process by which a credit card holder could register his personal car key may involve swiping the credit card, touching the RFID token, for example the car key, and presenting the credit card and signature, for validation by an attendant.

[0036] Invisible to the customer would be a pre-authorization check of the credit card, and registration of the card with the token's unique identification number. The registration will cause the particular credit card to become the default payment mechanism for the token. In addition to the signature check, other information could be captured at registration, e.g., social security number, mother's maiden name, address, car license plate number, etc. The goal of registering the token may be to obtain VISA, MasterCard, American Express, or other credit card approval that the

token is as secure as a card present transaction and thus entitled to the same interchange. Additionally, registering the token may occur in a closed loop environment, where an outside financial network, such as credit card network, is not involved.

[0037] Central controller 114 of FIG. 1 also provides an interface between network 102 and account storage 116. Information from reader 104 and/or register/reader 112 is transmitted to central controller 114 to be stored in account storage 116. Information to be stored may include details regarding the purchase transaction, as well as other statistics. For example, purchase transaction information may be stored in account storage 116 for a set period of time, and then communicated to token account storage 110 to finalize the purchase transaction (e.g., daily, weekly, monthly, etc.). Alternatively, account storage 116 may communicate directly with funding sources 120 to finalize the purchase transaction.

[0038] The invention encompasses a means by which a consumer can register his RFID car key, to permit him to authenticate himself to a payments network and to execute payment transactions. Registration might be as simple as swiping his credit card, and immediately subsequently having his car key's RFID number read. At the same time, the owner of the car key can be asked for pertinent personal information. Some credit card companies may be more comfortable if the consumer executes a signature at the same time. A further means of assuring the correct user is registered would be to mail a temporary PIN to the credit cardholder's home address. Another means to verify the registration might be to validate with the department of motor vehicles that the registrant is in fact an owner of the specified vehicle. With one card registered to the RFID car key, it should be easy asynchronously to register his other bank/credit cards, so long as the mailing address is the same.

[0039] FIG. 3 is a flow chart illustrating a process for performing token and account registration according to an embodiment of the invention. At step 305, an RFID device is activated. Although the example illustrated in FIG. 3 used an RFID device as the token, it is understood that other types of tokens may also be used. Activation of an RFID device may include transmitting a signal to a passive RFID device, communicating with a server, or activating the appropriate power source in an active RFID device. According to an embodiment of the invention, activation of the token, such as an RFID device, occurs when the server recognizes the RFID device, thereby enabling purchase transactions and other transactions to be performed. While the process illustrated in FIG. 3 discloses certain steps performed in a particular order, it should be understood that the present invention may be practiced by adding one or more steps to the process, omitting steps within the process, and/or altering the order in which one or more steps are performed.

[0040] At step 310, the unique identification identifier is read, and an account is created for the RFID device at step 315. The terms of the account are established at step 320, and the account information is stored at step 325. Terms may include permissions to use the account, the amount of the purchase transaction authorization for the account, the priority of the account if more than one financial account is associated with the RFID device, or other terms for performing the purchase transaction. By way of illustrative

example, terms for a particular account may include authorizing purchase transactions under a particular amount without requiring a validation or confirmation. By way of another illustrative example, certain accounts may not be valid at certain times of the day, or for certain merchants. By way of a further illustrative example, one account may be set as a default, such that unless otherwise selected by the user of the RFID device, the default financial account will be used to perform the purchase transaction. Other terms may also be used. By way of another example, certain transactions may be performed using a specific financial account (e.g., under \$50) or those made at specific merchants or types of merchants (e.g., purchases at gas stations).

[0041] A financial account is registered at step 330. Financial accounts may include credit card accounts, bank accounts, debit accounts, or other type of monetary accounts direct or indirect. The financial account is associated with the RFID device and the unique identifier at step 335. By associating a financial account with the RFID device and the unique identifier, the financial account may be used to perform a purchase transaction.

[0042] At step 340, the terms of the financial account are established. The terms for the financial account may be the same as those set forth above. At step 345, the information for the financial account is stored. At step 350, a determination is made whether additional financial accounts are to be registered with the RFID device. If yes, the process returns to step 330 to register the financial account. If not, the process ends at step 355.

[0043] FIG. 4 is a flow chart illustrating a process for performing token and account registration according to an embodiment of the invention. At step 405, an RFID device is activated. Although the example illustrated in FIG. 4 used an RFID device as the token, it is understood that other types of tokens may also be used. Activation of an RFID device may include transmitting a signal to a passive RFID device, activating at a server or activating the appropriate power source in an active RFID device. While the process illustrated in FIG. 4 discloses certain steps performed in a particular order, it should be understood that the present invention may be practiced by adding one or more steps to the process, omitting steps within the process, and/or altering the order in which one or more steps are performed.

[0044] At step 410, the unique identification identifier is read. At step 415, the network protocol used for the particular purchase transaction is determined. According to an embodiment of the invention, different readers may operate on the same frequency, but use different protocols. A token, such as an RFID device, may be programmed in a specific protocol, and the reader may be programmed to determine what protocol is being used and process the information accordingly.

[0045] The purchase amount is generated at step 420. At step 425, the purchase transaction is authorized. Authentication may include inputting a PIN, providing bio-metric information, inputting a password, or other manner of authentication. Once authenticated, authorization may include confirming that a purchase transaction has been approved. According to an embodiment of the invention, authorization may be completed when the token is authorized at the server, such as central controller 108. As described previously in reference to FIG. 1, authentication

list 118 determines if reader 104 and/or token 106 is authentic and permitted to perform transactions. Authentication list may be used as security to reduce the chances of fraud. According to an embodiment of the invention, token 106 may include information about the address (e.g., internet address) of central controller 108. Reader 104 may then access central controller 108 to perform the purchase transaction. Authentication list 118 may be accessed to ensure that token 106 is allowed to perform a transaction. For example, authentication list 118 may contain a list of tokens 106 that are in good standing, or that are delinquent. While FIG. 1 illustrates authentication list 118 in communication with central controller 108, it is understood that authentication list 118 may be in communication with or resident on reader 104 and/or register/reader 112. Authentication list 118 may also ensure that reader 104 is allowed to access central controller 108. According to an embodiment of the invention, authentication list 118 may also include a list of authorized readers and register/readers that are permitted to access central controller 108.

[0046] At step 430, a determination is made whether more than one financial account is associated with the RFID device. If only one financial account is associated with the RFID device, the account is charged for the purchase transaction at step 435. The account may be charged using any conventional process, such as that used for credit card and debit card transactions. Other manners for charging an account may also be used.

[0047] At step 450, the purchase transaction is then finalized. Finalizing the purchase transaction may include printing a receipt, confirming that the transaction has been made, or other steps used to conventionally finalize a purchase.

[0048] If there is more than one financial account associated with the RFID device, an account is selected at step 440 and the selected account is charged for the purchase transaction at step 445. Selecting an account may involve the user of the RFID device selecting the particular account, or, if no selection has been made, selecting the account designated as the default account. The account may be charged using any conventional process, such as that used for credit card and debit card transactions. Other manners for charging an account may also be used.

[0049] In the process of seeking authorization for a particular transaction, the account specified to be debited may not have adequate resources to cover the transaction. In that event, whether the account was funded on a pre-pay or post-pay basis, the Central Controller 108, could: (i) by prior arrangement, automatically top-up the account with additional resources by seeking additional credit/funds from a specified account; (ii) seek funds from any other default funding/credit accounts; or (iii) reject the transaction. Other processes may also be used.

[0050] Again, at step 450, the purchase transaction is then finalized. Finalizing the purchase transaction may include printing a receipt, confirming that the transaction has been made, or other steps used to conventionally finalize a purchase. The process then ends at step 455.

[0051] In addition to using the RFID car key or other token for making payments, the same authentication mechanism is useful generally to validate one's identity. For example, the RFID car key can be used to authenticate oneself to a virtual

private network ("VPN"), or other secure networks, for physical access to premises, for buying and selling securities or other non-payment transactions, for purposes of time-cards, for loyalty programs, or to one's medical insurer. The token can be used both with and without PIN, bio-metric, passwords or other identification confirmations. For lower value transactions, a consumer might choose the convenience of not requiring a PIN. For larger transactions, a consumer may choose to require the use of a PIN or bio-metric information.

[0052] Using a single device for multiple purposes will be much more convenient for consumers, who can begin to skinny down their wallets. If the token is lost, it is also easier for the consumer to revoke all his powers at once. The consumer can simply revoke the token's authorities and instantaneously all the powers of the token will be lost. As relevant information is already available, re-registering is eased as the new token need only be associated with the financial accounts.

[0053] Currently, most RFID devices operate at around 134 kHz. However, a new generation of RFID devices may operate at other frequencies, such as 13 MHz. Higher frequency devices may be less expensive to build and will permit higher bandwidth (i.e. quicker) communications. About 70% of the 40 million cars produced in 2001 were equipped with RFID anti-theft systems. The cars have an RFID reader in the ignition switch. Unless the electronic engine controller recognizes the car key's RFID token, the car will not start. According to an embodiment of the invention, various aspects of the RFID car keys make them useful as payment devices. First, each key has a unique ID number. Such car keys protect the owner's unique number much more securely than a magnetic stripe card. Second, there is a single, standard protocol that permits RFID readers to access the unique number on all RFID chips. Thus, standard RFID readers permit ordinary car keys to become trusted hardware authentication tokens. After a simple registration process, consumers may use their car keys to make payments at any store with an ordinary RFID reader.

[0054] According to an embodiment of the invention, a primary registration may require the physical presence of the token. Additional credit cards and other financial accounts with the same name and billing address could be added to the token at a registration station merely by swiping the new credit card and touching the token, one-after-the-other. Subsequent cards could also be added online, or by using a VRU (though security may require some additional identification information).

[0055] Token owners can choose to use any of their available payment mechanisms at any merchant, and the owner's payment choices can be changed easily. The owner will make payment elections online or over a VRU and will be able to specify the mode of authentication required for different types of transactions, e.g. require a PIN for online or larger payments.

[0056] A token, such as an RFID device, will be accepted at any merchant that takes any RFID payments. In the simplest case, a consumer will simply bring the token close to the reader at checkout. The reader will automatically debit the payment account specified by the consumer. Consumers may specify more than one payment mechanism for a merchant. In that case, a merchant's payment wizard will

select the payment mechanism with the lowest merchant discount. If the consumer has not specified a particular payment mechanism for a merchant, the default payment method will be charged.

[0057] Online purchases are also possible when a computer is equipped with an RFID reader. The incremental cost of adding that functionality to a personal computer ("PC") may be minimal. With a widely deployed base of tokens, RFID enabled PCs can offer very substantial benefits in addition to secure payments. PCs equipped with RFID readers could be used to secure data on the PC, to access secure networks, for VPNs, for remote access, etc.

[0058] According to an embodiment of the invention, consumers may be able selectively to impose additional security protections. A PIN may be required for purchases at specific stores, or for amounts larger than a specified ceiling. Consumers may also choose to impose a daily or weekly maximum aggregate spending limit. Subordinate tokens may be restricted to purchases from specific stores, or for age appropriate materials (especially useful for online purchases).

[0059] By way of an example of an embodiment of the invention, a car might be sold with one master token, registered as the property of the owner of the car. Using the master token, the owner of a car might create, authorize or reject driving privileges, payment capabilities, etc., for other users of tokens to his car. The master token holder might act as the registration agent for subordinate tokens, and could also be empowered to revoke or suspend the powers for subordinate tokens. An additional validation check before registering a master token might be to compare the credit card billing address with the address of the registered owner of the vehicle.

[0060] Similarly, a token might be registered to the owner of a house fitted with an electronic RFID lock. The house master token could be used to register other authorized users of the house. Such registration might be very simple, e.g., touch the house master token, insert a PIN and then touch the subordinate token. Subordinate tokens might have time-limited efficacy, e.g., a teenager's token might not work after his curfew.

[0061] One aspect of the RFID functionality is their use for personalization, as well as for heavier payments and authorizations. Readers are not bound by the same constraints as the passive RFID devices (size, cost, etc.). Typical RFID readers will have some source of power and be connected to some device, network, or system that takes advantage of the RFID validation, e.g., POS, EPoS, ECR, fire wall, engine controller, physical lock to premises, etc.. The RFID reader may be equipped with an antenna tuned to listen for faint signals at a specific frequency, e.g., 134 kHz. More complex RF communications could simply be enabled with software. The two-way, secure communication could use RF (with the same frequency as the passive RFID device or a different one), or other protocols such as Bluetooth or 802.11.

[0062] One manner for expanding the functionality of the passive RFID device is to link its powers to an active device. Such devices might include a wire line or cellular phone, computer, Blackberry, PDA or other similar device (hereinafter also referred to as "Active Communications Device").

Such Active Communications Devices typically have power, or access to power, one or more communications channels, a CPU that is much more powerful than the passive RFID, memory that can be dynamically accessed, data entry capability and a visual display. The passive RFID token that is validated might be electrically connected to the Active Communications Device; physically attached, but not electrically connected, e.g. RFID chip embedded in the faceplate of a cell phone; or, separate from the Active Communications Device. For example, when an Active Communications Device is a mobile telephone, an RFID device may be located in face plate of the telephone. The RFID device may be a passive device, and the mobile telephone may have an RFID reader. The mobile telephone then communicates the necessary information. Alternatively, the RFID device may be physically connected to the mobile telephone, such as by electrical leads. The link between the RFID and the Active Communications Device may be established at the manufacturer, or later, by direct or indirect contact with registration authority, or over a network. Other embodiments may also be used.

[0063] Once an authenticated passive RFID is recognized and accepted by an RFID reader, the holder of the RFID device could take advantage of that trusted authentication, to engage an active device capable of more complex, secure communications. The key step to achieve this result will be to transfer the passive RFID's trusted validation, to a more capable communications device. There are many different ways for that trust to be transferred, three different examples are disclosed here.

[0064] While two examples for linking, by prior arrangement, an authenticated passive RFID device to an Active Communications Device are disclosed below, it is understood that other examples are also within the scope of the present invention.

[0065] Just as a passive RFID device can be registered to enable multiple payments modes (e.g., credit cards, debit and stored value accounts, etc.), and other non-payment authorizations; RFID devices can be securely linked to other devices, including Active Communications Devices. By registering a passive RFID device with an Active Communications Device's unique identifier, that Active Communications Device can inherit all the authentication and authorization capabilities of the passive RFID device. Thereafter, the holder of a passive RFID device could use it wherever it is convenient (e.g., where a merchant's POS is capable only of recognizing a passive RFID device) and would also use the same set of capabilities using his Active Communications Device to take advantage of less limited reader capabilities where available.

[0066] In the case of automotive security, during secure instantiation of each token, the engine controller communicates its secret to the token. The engine controller will start the car only for 'friendly' tokens that know its secret. For example, controller A (the engine controller) shares its secret with token B (the token). Because controller A controls distribution of its secret, controller A will trust all token Bs that know its secret.

[0067] To establish a link between a passive RFID device and an Active Communications Device that can be trusted by RFID readers may be somewhat more complex. The Active Communications Device may securely share its

secret with the passive RFID device in a manner similar to the way engine controllers instantiate tokens and in a carefully controlled circumstance. The passive RFID device subsequently may communicate to a reader both the RFID device's unique identifier number and the secret shared with the Active Communications Device. The RFID reader may then trust communications with the Active Communications Device that identified itself with the same RFID secret. Alternatively, the Active Communications Device could be certified by a payment authority entrusted to pass RFID information for payment authorization.

[0068] The RFID reader validates and then trusts the authenticated passive RFID device. The authenticated passive RFID device separately communicates to the RFID reader a secret. The RFID reader then can trust the Active Communications Device and knows that the authenticated passive RFID device's secret. Based on the security model, the trust can be time limited (e.g. where the RFID reader will recognize the Active Communications Device only when the authenticated passive RFID device and C are used contemporaneously), or not. In addition, the reverse mechanism can also work, where the authenticated Active Communications Device is linked to a passive RFID device. In a manner similar to the engine controller, an Active Communications Device might share its secret with the passive RFID device.

[0069] Linkage of a passive RFID device to an Active Communications Device by prior arrangement may be useful when that linkage is intended to be persistent. There are circumstances where such persistence is not desirable. For example, suppose in the future a driver rents a car and wishes to use his passive RFID token to pay tolls. Rental cars are used by many different people, persistent linkage of RFID devices personal to drivers present problems for such temporary connections. One means to provide for payment of tolls would be to take advantage of the driver's payment capability, by simply using a car's transmitter to broadcast that capability to the toll collectors. The system would work so long as the car validates the drivers ability to pay and is trusted as a payment agent or the transmitter can directly pass the driver's credentials.

[0070] Small, relatively inexpensive toll tags permit cars to be recognized and charged for tolls while traveling as fast as 200 MPH. Toll tags are active RFID devices, with batteries and the ability to transmit signals. Across the country, there are a plethora of divergent toll tag protocols that are not interoperable. It would be cheap and easy to build a single, multi-purpose electronic device to permit cars to communicate with all the various toll tag readers. If the car could authenticate a driver's ability to pay, drivers might travel across the country without ever stopping to pay cash for tolls.

[0071] Drivers could individually register with each different toll authority, or execute a single, multi-registration that covers many toll authorities. The toll registration could provide for a single stored value account, which would automatically be debited by each of the various toll authorities and topped-up using a single source of payment. The payment account could be linked to a single RFID device.

[0072] For each car enabled with the universal toll transmitter, drivers could authenticate themselves with their personal RFID token, and proceed through the speedier toll tag lines, no muss no fuss. Since most new cars already have

RFID readers, it would be quite easy to enable a second site convenient to permit drivers to authenticate their passive RFID devices.

[0073] If a passive RFID device has a broadly accepted payment mechanism attached, sometimes prior registration with the toll authorities might be avoided. The toll collector could optimistically accept the RFID number, and seek payment. Photographing the license plate or some similar mechanism could provide anti-fraud protection.

[0074] According to an embodiment of the invention, the systems and processes described in this invention may be implemented on any general or special purpose computational device, either as a standalone application or applications, or even across several general or special purpose computational devices connected over a network and as a group operating in a client-server mode. According to another embodiment of the invention, a computer-usable and writeable medium having a plurality of computer readable program code stored therein may be provided for practicing the process of the present invention. The process and system of the present invention may be implemented within a variety of operating systems, such as a Windows® operating system, various versions of a Unix-based operating system (e.g., a Hewlett Packard, a Red Hat, or a Linux version of a Unix-based operating system), or various versions of an AS/400-based operating system. For example, the computer-usable and writeable medium may be comprised of a CD ROM, a floppy disk, a hard disk, or any other computer-usable medium. One or more of the components of the system or systems embodying the present invention may comprise computer readable program code in the form of functional instructions stored in the computer-usable medium such that when the computer-usable medium is installed on the system or systems, those components cause the system to perform the functions described. The computer readable program code for the present invention may also be bundled with other computer readable program software. Also, only some of the components may be provided in computer-readable code.

[0075] Additionally, various entities and combinations of entities may employ a computer to implement the components performing the above-described functions. According to an embodiment of the invention, the computer may be a standard computer comprising an input device, an output device, a processor device, and a data storage device. According to other embodiments of the invention, various components may be computers in different departments within the same corporation or entity. Other computer configurations may also be used. According to another embodiment of the invention, various components may be separate entities such as corporations or limited liability companies. Other embodiments, in compliance with applicable laws and regulations, may also be used.

[0076] According to one specific embodiment of the present invention, the system may comprise components of a software system. The system may operate on a network and may be connected to other systems sharing a common database. Other hardware arrangements may also be provided.

[0077] Other embodiments, uses and advantages of the present invention will be apparent to those skilled in the art from consideration of the specification and practice of the

invention disclosed herein. The specification and examples should be considered exemplary only. The intended scope of the invention is only limited by the claims appended hereto.

[0078] While the invention has been particularly shown and described within the framework of performing purchase transactions using a token from an automobile, it will be appreciated that variations and modifications can be effected by a person of ordinary skill in the art without departing from the scope of the invention. For example, one of ordinary skill in the art will recognize that various types of tokens may be used to perform purchase transactions and that other types of transactions may also be performed using a token. Furthermore, one of ordinary skill in the art will recognize that such processes and systems do not need to be restricted to the specific embodiments described herein.

1. A system for performing at least one payment transactions comprising:

a token having a unique identifier associated with a particular automobile, where the automobile is held out as a trusted entity and the token interacts with a reader to perform the at least one payment transaction; and

at least one account associated with the token, where the at least one account makes payments as directed by interaction of the token and the reader.

2. The system according to claim 1, where the token is a radio frequency identification device.

3. The system according to claim 2, where the radio frequency identification device is an active device.

4. The system according to claim 2, where the radio frequency identification device is a passive device.

5. The system according to claim 1, where the token reader is associated with a toll-road payment system.

6. The system according to claim 1, where an authorization indicia is required for the purchase transaction to be performed.

7. The system according to claim 1, where at least one credit card is registered to the token.

8. The system according to claim 7, where the at least one account is funded by a transfer funds from the at least one registered credit card to the at least one account.

9. The system according to claim 1, where the at least one account is a credit card account registered with the token.

10. The system according to claim 1, where at least one financial account is registered to the token.

11. The system according to claim 10, where the at least one account is funded by a transfer funds from the at least one registered financial account to the at least one account.

12. The system according to claim 1, where the at least one account is a financial account registered with the token.

13. A system for registering a token, comprising:

means for receiving a unique identifier from the token, where the token and the unique identifier are associated with a user or a key of a particular automobile, the automobile is held out as an entity trusted by a merchant and the token interacts with a reader to perform the at least one payment transaction;

means for creating at least one account associated with the token, where the account includes account information and makes payments as directed by interaction of the token and the reader;

means for receiving terms for the at least one account; and

means for storing the account information and the terms of the at least one account.

14. The system according to claim 13, where the token is a radio frequency identification device.

15. The system according to claim 14, where the radio frequency identification device is an active device.

16. The system according to claim 14, where the radio frequency identification device is a passive device.

17. The system according to claim 13, where the token reader is associated with a toll-road payment system.

18. The system according to claim 13, where an authorization indicia is required for the purchase transaction to be performed.

19. The system according to claim 13, where at least one credit card is registered to the token.

20. The system according to claim 19, where the at least one account is funded by a transfer funds from the at least one registered credit card to the at least one account.

21. The system according to claim 13, where the at least one account is a credit card account registered with the token.

22. The system according to claim 13, where at least one financial account is registered to the token.

23. The system according to claim 22, where the at least one account is funded by a transfer funds from the at least one registered financial account to the at least one account.

24. The system according to claim 13, where the at least one account is a financial account registered with the token.

25. A process for registering a token, comprising:

receiving a unique identifier from the token, where the token and the unique identifier are associated with a user or a key of a particular automobile, the automobile is held out as an entity trusted by a merchant and the token interacts with a reader to perform the at least one payment transaction;

creating at least one account associated with the token, where the account includes account information and makes payments as directed by interaction of the token and the reader;

receiving terms for the at least one account; and

storing the account information and the terms of the at least one account.

26. The process according to claim 25, where the token is a radio frequency identification device.

27. The process according to claim 26, where the radio frequency identification device is an active device.

28. The process according to claim 26, where the radio frequency identification device is a passive device.

29. The process according to claim 25, where the token reader is associated with a toll-road payment system.

30. The process according to claim 25, where an authorization indicia is required for the purchase transaction to be performed.

31. The process according to claim 25, where at least one credit card is registered to the token.

32. The process according to claim 31, where the at least one account is funded by a transfer funds from the at least one registered credit card to the at least one account.

33. The process according to claim 25, where the at least one account is a credit card account registered with the token.

34. The process according to claim 25, where at least one financial account is registered to the token.

35. The process according to claim 34, where the at least one account is funded by a transfer funds from the at least one registered financial account to the at least one account.

36. The process according to claim 25, where the at least one account is a financial account registered with the token.

37. A computer readable medium having code for causing a processor to register a token, comprising:

code for receiving a unique identifier from the token, where the token and the unique identifier are associated with a particular automobile, the automobile is held out as a trusted entity and the token interacts with a reader to perform the at least one payment transaction;

code for creating at least one account associated with the token, where the account includes account information and makes payments as directed by interaction of the token and the reader;

code for receiving terms for the at least one account; and

code for storing the account information and the terms of the at least one account.

38. The medium according to claim 37, where the token is a radio frequency identification device.

39. The medium according to claim 38, where the radio frequency identification device is an active device.

40. The medium according to claim 38, where the radio frequency identification device is a passive device.

41. The medium according to claim 37, where the token reader is associated with a toll-road payment system.

42. The medium according to claim 37, where an authorization indicia is required for the purchase transaction to be performed.

43. The medium according to claim 37, where at least one credit card is registered to the token.

44. The medium according to claim 43, where the at least one account is funded by a transfer funds from the at least one registered credit card to the at least one account.

45. The medium according to claim 37, where the at least one account is a credit card account registered with the token.

46. The medium according to claim 38, where at least one financial account is registered to the token.

47. The medium according to claim 46, where the at least one account is funded by a transfer funds from the at least one registered financial account to the at least one account.

48. The medium according to claim 37, where the at least one account is a financial account registered with the token.

* * * * *