

SYSTEMS AND METHODS FOR USING IDENTITY DOCUMENTS TO MAKE PURCHASES

TECHNICAL FIELD

[0001] The technical field comprises electronic funds transfer. The technical field also comprises electronic funds transfer with electronic mechanisms providing security. The technical field also comprises point of sale terminals.

BACKGROUND

[0002] Carrying cash can be inconvenient due to bulk, and risk of loss or theft. Credit cards and debit cards are known in the art. Debit cards can be used by customers at point of sale terminals to purchase goods or services. A personal identification number or PIN is usually entered by the customer at a reader after the card has been swiped at the reader. If the PIN entered matches the PIN on record, the transaction is approved.

[0003] Student cards that are used for student dining and that can also be used with area merchants are also known. For example, the Eagle Card offered by Eastern Washington University acts as student ID and can be used for access to university facilities such as the library, gym, computer labs, and sports events. The Eagle Card can also be used in an EagleFlex prepaid declining balance program for meals in university dining halls, as well as to purchase goods and services from area merchants. Funds can be added if a student or parent desires that the card be useable for purchases as opposed to as just a student ID card. Cash withdrawals are not permitted. The Eagle card and EagleFlex program are described at <http://access.ewu.edu/EagleCard/General-Information.xml>

[0004] Similarly, Marist College provides a card that is a personal college identification card that acts as a college library card, that grants students admission to college activities and events, that grants check cashing privileges at Marist College, is a dining service card, and that secures residence hall access. The Marist card can also be used to purchase goods and services from off campus merchants. The Marist card can be loaded with Marist Money that can be used with participating off-campus merchants, including restaurants, grocery stores and other retail stores. Marist Money accounts can be debited for telephone orders by entering the card number manually into a terminal but, in case of a dispute, the burden of proof lies with the merchant and

it is recommended that a cardholder's authorization signature be obtained.

Restrictions exist on the types of goods and services that can be purchased; e.g., Marist Money cannot be used for the purchase of alcohol, illicit drug paraphernalia, lottery tickets or for card-to-cash exchange (i.e. merchants may not accept Marist Money in exchange for cash). In exchange for services such as marketing and operation of the program, each merchant pays a 5% service charge on all gross Marist Money sales. Each merchant is also required to rent a transaction terminal or reader and must also provide a telephone line for the transaction terminal or reader. The college reimburses merchants for gross sales minus the 5% commission by check every 30 days, which is provided along with a statement.

[0005] U.S. Patent Application Publication 2007/0150413 to Morgenstern discloses an e-commerce system for creation and management of electronic currency. The system includes a database that maintains a list of merchant and customer accounts. Respective accounts have an assigned amount e-commerce currency units called UNEEs and identification information about the merchants or customers who own the accounts. The electronic currency units are purchased by respective customers for placement into their accounts. Payments in UNEEs for purchases by a customer result in a transfer of electronic currency from the customer's account to the merchant's account. Payments received by the merchant can be retained as UNEEs, or can be converted into a national currency or other asset of value selected by the merchant. UNEE transactions between a customer and a merchant result in a request to the database system with instructions to transfer the desired number of UNEEs between accounts. The availability of the UNEEs is verified by the central database system, and if funds are available, the UNEEs are transferred.

SUMMARY

[0006] An organization, body, employer or plan administrator, in certain embodiments, preselects a list of users, customers, or employees to be given an amount of credit points to be used in retail stores for a validity period. These credit points are distinct from legal tender such as cash and credit and are to be used for purchase of items in retail stores. Retail point of sale software on the market often does not cater to such transactions. Thus, various embodiments provide systems and methods to allow a list of pre-selected customers authorized by the organization to

iteratively use the credit points for purchases while providing a measure or measures to validate the consumer.

[0007] Some embodiments provide a server comprising:

- a processor, memory, and a data bus, and configured to execute a multi-tasking, multi-user operating system supporting multiple simultaneous sessions;

- a network adapter coupled to the processor and configured to receive a connection from a point of sale terminal; and

- a database coupled to the processor and arranged to associate identification cards with respective electronic accounts for customers, the database including entries for customer identifiers, account codes for respective customers, amount of credit points in respective accounts, fingerprints and secret codes for respective accounts;

- the server being configured to add credit points to one of the accounts on a periodic basis;

- the server being configured to receive an inquiry as to the amount of credit points in the account of a first one of the customers from a first one of the point of sale terminals, the inquiry including customer information data, the server being configured to retrieve information representing the amount of credit points in the first cardholder's account from the database, and to send the amount of credit points in the first cardholder's account to the first point of sale terminal;

- the server being configured to receive, from the first point of sale terminal, a request to validate the customer for conclusion for a sale transaction, the request including a customer identifier and at least one of a customer secret code and customer fingerprint, the server being configured to compare the secret code from the point of sale terminal to the secret code in the database associated with the customer identifier and, if there is a match, to validate the customer; and

- the server being configured to receive, from the first point of sale terminal, a request to deduct credit points from the account of the validated customer, the request to deduct resulting from a purchase of items at the first point of sale terminal and the request to deduct including an amount of points based on the cost of the purchase items and information identifying the account of the validated customer.

[0008] Some embodiments provide method comprising:

associating an identification card, issued from an organization to persons, with respective electronic accounts for at least some of those persons in a database in a server, the database including entries for the persons, accounts for respective of the persons, credit points in respective accounts, and personal identification numbers for respective accounts, the identification cards bearing data capable of being read by a point of sale device, the data identifying the persons holding the respective cards;

periodically depositing credit points in the account of a first one of the persons by changing data in the database;

receiving an inquiry as to the amount of credit points in the account of the first person from a point of sale device;

retrieving information representing the amount of credit points in the first person's account from the database using a dedicated line between the point of sale device and the server;

returning the amount of credit points in the first person's account to the point of sale device;

determining, at the point of sale device, the amount of credit points required for a purchase of goods or services by the first person;

determining if the amount of credit points in the first person's account is at least as much as the amount of credit points required and, if not, inquiring at the point of sale device as to whether the first person would like to pay using a mix of cash and credit points;

requesting that the first person enter his personal identification number or fingerprint at the point of sale device and receiving a request, at the point of sale device, to deduct a number of credit points from the first person's account; and

receiving the entered personal identification number or fingerprint, using the dedicated line, and querying the database, to determine if the entered personal identification number matches the personal identification number in the database for the first person's account and, if so, deducting the requested number of credit points from the first person's account in the database.

[0009] Some embodiments provide a non-transitory computer readable medium bearing computer program code that, when executed in a computer causes the computer to:

define a database including entries for customer identifiers, account codes for respective customers, amount of credit points in respective accounts, fingerprints and secret codes for respective accounts;

receive an inquiry as to the amount of credit points in the account of a first customer from a point of sale terminal, the inquiry including customer information data;

retrieve information representing the amount of credit points in the first cardholder's account from the database;

send the amount of credit points in the first cardholder's account to the point of sale terminal;

receive, from the point of sale terminal, a request to validate the customer for conclusion for a sale transaction, the request including a customer identifier and a customer secret code or fingerprint;

compare the secret code or fingerprint from the point of sale terminal to the secret code or fingerprint in the database associated with the customer identifier and, if there is a match, validate the customer; and

receive, from the point of sale terminal, a request to deduct credit points from the account of the validated customer, the request to deduct resulting from a purchase of items at the point of sale terminal and the request to deduct including an amount of points based on the cost of the purchase items and information identifying the account of the validated customer.

BRIEF DESCRIPTION OF THE VIEWS OF THE DRAWINGS

[0010] FIG. 1A is a block diagram of a system in accordance with various embodiments.

[0011] FIG. 1B is a block diagram of a point of sale system in accordance with various embodiments.

[0012] FIG. 2 is a flowchart illustrating operation of a system such as the system of FIGS. 1A and B, in accordance with various embodiments.

[0013] FIG. 3 is a flowchart illustrating additional details for one of the blocks of FIG. 2, in accordance with various embodiments.

[0014] FIG. 4 is a flowchart illustrating additional details for one of the blocks of FIG. 2, in accordance with various embodiments.

DETAILED DESCRIPTION OF THE ILLUSTRATED EMBODIMENTS

[0015] Systems and methods of deducting credit points from a customer account are provided. In some embodiments, a request to retrieve customer available credit points is received from a point of sale terminal. The request includes account identification data associated with the customer account. The customer account identification data is entered at a point of sale terminal or device. In some embodiments, the amount of customer available credit points is retrieved and displayed to the customer. In some embodiments, the amount of available credit points is displayed together with customer identification data. A request to validate the customer at the end of a sale transaction is received from the point of sale terminal. The request includes a customer secret code associated with the customer identification data. An indicator on the validity of the secret code is returned to the point of sale device. In some embodiments, a request to deduct credit points from a customer's account is received from a point of sale system at the end of a sale transaction after the secret code is validated. In some embodiments, the request includes credit points and account identification data associated with the customer account. The credit points are deducted from the customer account. In some embodiments, subsequent credit point purchase transactions will continue to cause the credit points to be deducted, such as until the credit points are fully utilized.

[0016] Pre-selected customers associated with an organization are given some credit points to be used in various retail stores specially setup for these customers, in some embodiments. Various embodiments provide a process that allows the customer to deduct credit points, i.e., corresponding to the value of purchased items, from an existing customer account stored in a central system or server from a point of sale (POS) terminal, device, or system.

[0017] FIG. 1A shows a system 10 in accordance with various embodiments. The system 10 includes a server 12 including one or more processors 14 having one or more cores each, memory such as RAM 16, ROM 18, long term storage or memory 20 in the form of one or more hard drives or solid state drives or both, a data bus, and other components typical of web servers. Fault tolerant features such as multiple

redundant power supplies and memory arranged in RAID arrays may be employed. The server 12 is configured to execute a multi-tasking, multi-user operating system supporting multiple simultaneous sessions.

[0018] The server 12 further includes one or more network cards or adapters 22 and 24 coupled to the processor and configured to receive connections from point of sale terminals, systems or devices 26, 27, 28, and 29 over a communication link 32. In the illustrated embodiment, the communication links 32 comprise dedicated lines 32 (e.g., leased lines or dial-up). In some embodiments, transfer of data between a point of sale terminal 26-29 and the server 12 is via web service.

[0019] In some embodiments, the system 10 further includes one or more firewalls 36 between the server 12 and the point of sale terminals 26-29. The firewall 36 is defined by separate hardware in some embodiments, and by software loaded in the server in other embodiments.

[0020] The system 10 further includes a database 38 coupled to the processor 14. The database 38 may be defined in the long term storage 20. Alternatively, the database 38 may be external to a housing containing the processor 14, RAM 16, and ROM 18. For example, the database 38 may be stored in another computer or server or in an external hard drive or SSD. The database 38 is arranged to associate identification cards with respective electronic accounts for customers or cardholders. More particularly, in some embodiments, the database 38 at least includes entries for customer or cardholder identifiers 40, amount of credit points 44 in respective accounts, and secret codes 46, for respective accounts. In some embodiments, the secret codes or other data is masked off or not stored as clear text. In some embodiments, personal identification numbers (PINs) are used for the secret codes 46. In some embodiments, the database 38 further includes entries 47 for (or pointing to) images of fingerprints for respective cardholders. The fingerprints can be used as an alternative to a PIN, such as in case a customer forgets his or her PIN.

[0021] In some embodiments, additional entries are included in the database 38. For example, in some embodiments, entries are included for account codes 42 for or identifiers 40 (or both) for respective customers. In some embodiments, account codes 40 comprise employee numbers assigned by a company or member IDs of an organization. In some embodiments, account codes 42 comprise National Registration Identity Card ("NRIC") numbers or other types of national identification

numbers or codes. The NRIC is an identity document that is in use in Singapore. Unlike a Passport, an NRIC is about the size of a credit card and can be carried around with ease. It is issued by the Immigration & Checkpoints Authority (ICA) to Singaporean citizens and permanent residents who are fifteen years of age and older. Each NRIC is identified by an NRIC number ("Identity Card Number"), which is a unique set of nine alpha-numerics. It is mandatory for such citizens and permanent residents to bring the NRIC wherever they go - as a form of identification; e.g. during checks by police. The NRICs include information identifying the owner of the card, such as holder's name, race, date of birth, sex, country of birth, a photograph, the NRIC number, a bar code, a fingerprint, issue date of the card, and the holder's residential address. The NRICs can be used to borrow books from the public libraries (library cards are no longer necessary in Singapore). In other embodiments, other forms of unique identification can be employed such as the employee number on an employee pass. An employee pass is typically the size of a credit card and normally has a photo of an employee and is barcoded (or has a magnetic strip encoded) with the employee number. In some embodiments, entries 48 are included indicating whether an account is active. In other embodiments, entries are included indicating date of last use, and if that date is more than a predetermined amount of time in the past, the account is considered to be inactive. In still other embodiments, if a customer's identifier 40 or account code 42 cannot be found in the database 38, the customer is considered to be an inactive customer.

[0022] In some embodiments, gender 50 or other characteristics of customers are included in the database 38 for each customer. This characteristics information can be useful, for example, for targeted advertising or to make sure that goods purchased are suitable for a customer of the indicated gender (e.g., a prompt can be displayed on a point of sale device if a male customer attempts to purchase clothes for a female, or the transaction can be forbidden). Other embodiments are possible.

[0023] The stored-customer credit point accounts and the customer PIN may be managed by a third party.

[0024] FIG. 1B shows details of a point of sale system, in accordance with some embodiments. The point of sale terminals, systems, or devices 26-29 respectively include for example, in some embodiments, a cash register 52 including a processor 54 for making calculations and controlling operation, a memory 56 for storing data, a clock 58 for recording the times of transactions, an input 60 selectively coupled to a bar code scanner for scanning products (or cards such as employee passes or NRICs), an input 62 selectively coupled to a weight scale for weighing produce, a keypad 64 for a cashier, a cash drawer 66, a network interface 68 for communications to a store LAN or other computer network, a display 70 for showing items scanned and prices, and a printer 72 for printing a receipt. The point of sale systems 26-29 also respectively include, in some embodiments, a credit card or banking machine or terminal 74 (typically including a separate housing from the cash register 52) including a processor 76, a credit or debit card reader 78, a keypad 80 using which a customer can respond to prompts relating to credit or debit card use, a network interface 82 for communications to a banking network, and a display 84 for showing prompts to a customer. A keypad 86 and fingerprint scanner 88 are also included for receiving secret codes 46 or fingerprints 47. The keypad 86 and fingerprint scanner 88 may be included in banking machine 74 or may be separate and otherwise in communication with the cash register 52. See, for example, U.S. Patents D333,147; 4,903,200; 6,625,579; 5,398,191 for examples of point of sale devices that can be employed in various embodiments. The Verifone VX510 is an example of a credit card machine or terminal that can be included in the point of sale devices 26-29.

[0025] FIG. 2 illustrates a method or process of operation 200 of a system such as the system 10 shown in FIG. 1A, in accordance with various embodiments.

[0026] The method 200 comprises, in various embodiments, in 202 issuing identification cards or documents to persons, cardholders or customers from an entity, body, administrator, employee benefits administrator, all hereinafter referred to as an organization. In some embodiments, the organization is a governmental organization, such as a national government and the cards are NRIC cards. In some embodiments, issuing cards comprises an employer or company issuing a company pass. This organization controls operation of the server 12 in some embodiments. In other embodiments, the server is administered by an organization different from the entity that issues the identification cards or documents. In some embodiments, the

organization that administers the server is an employer. In some embodiments, the identification cards bear data capable of being read by a point of sale device, the data identifying the cardholders holding the respective cards. For example, in some embodiments, the cards include magnetic strips or are smart cards including electronic chips or fastpay chips. In other embodiments, data identifying the customer is manually entered into the point of sale device by the customer or by a cashier. In these embodiments where data is manually entered, a physical card is not necessary. For example, in some embodiments, for a customer who did not bring a physical card for a purchase, data identifying the customer is manually entered and the customer's fingerprint is scanned, using fingerprint scanner 88, instead of a PIN being entered.

[0027] The method 200 further comprises, in various embodiments, (see FIG. 1A) associating the identification cards (represented by identifiers 40) with respective electronic accounts 42 for customers in the database 38. In some embodiments, the database 38 is accessible by the server 12 and the server 12 is administered by the organization.

[0028] In some embodiments, in 204 (see FIG. 2) credit points or credits 44 are deposited in the account of a customer. This can be done from time to time or periodically (e.g., monthly), such as in the case of an employee benefit, or can be done at irregular times due to special events. Depositing credit points is performed, in the illustrated embodiment, by changing data (e.g., credit points 44) in the database 38. In some embodiments, an audit trail exists for manual data changes.

[0029] In 206, an inquiry is received as to the amount of credit points in the account of the customer from a point of sale device 26-29 such as from point of sale device 28.

[0030] In some embodiments, a request from the customer to display available credit points must include the customer identifier 40 (e.g. NRIC) or account code 42 (e.g. employee number) representing the customer identity. The customer identifier 40 is sent to the server 12, e.g. via web service. The identifier 40 is checked in the database 38 for its existence. The server 12 retrieves customer account information which includes, for example, some or all of customer available credit points 44, name or identifier 40, gender 50 and customer status indicator 48.

[0031] In 208, in response to receiving the inquiry 206, information 44 is retrieved representing the amount of credit points in the customer's account 42 from the database 38 using the communication link 32 between the point of sale device 28 and the server 12, in some embodiments.

[0032] In 210, in response to the retrieving of information 208, the amount of credit points in the customer's account is returned from the server 12 to the point of sale device 28, in some embodiments. In some embodiments, the amount of credit points 44 is displayed on the point of sale device 28.

[0033] In 212, in some embodiments, a determination is made as to whether the customer is an active customer (e.g., by querying an entry 48 for the customer in the database 38). If so, the process continues to 214. If not, the customer is not allowed to pay for goods or services using points. An active customer with available credit points can commence a sales transaction at the point of sale device 28. In some embodiments, the determination of 212 can be performed as part of the receiving the inquiry 206. For example, in some embodiments, if the record does not exist in the database 38, the customer will be considered as an inactive consumer in 212 where credit points are not available to be used for a purchase.

[0034] In various embodiments, in 214 a computation or determination is made at the point of sale device 28 as to the amount of credit points required for a purchase of goods or services by the customer. This can include, for example, adding up or totaling the prices of multiple items scanned or entered at the point of sale device 28. Taxes are included in the sum in various embodiments.

[0035] In 216, a computation or determination is made as to whether the amount of credit points in the customer's account is at least as much as the amount of credit points required and, if not, at 218 an inquiry is made at the point of sale device as to whether the customer would like to pay using a mix of cash and credit points. The inquiry of 218 can be by way of a message displayed on the point of sale device 28 to the customer or cashier. If the customer has insufficient available credit points, the customer can choose to pay the balance amount via a different payment mode such as cash, nets, debit card, or credit card.

[0036] If the computed credit points required for the purchase are less than or equal to the available credit points for the customer or if the customer is willing to pay the balance in cash in response to the inquiring 218, the method proceeds to 220 in various embodiments.

[0037] In various embodiments, in 220, a request is received, at the point of sale device 28, to deduct a number of credit points from the first customer's account. This may include a request that the customer enter his personal identification number or secret code 46 or fingerprint 47 at the point of sale device 28 and include receiving the personal identification number or secret code 46 at the point of sale device 28. In some embodiments, the receiving of the request of 220 occurs at the end of a sales transaction, at the stage where the total purchased value is determined. The purpose of the request to send the customer identifier 40 and the secret code 46 to the server 12 is to validate the customer, in some embodiments.

[0038] In various embodiments, in 224, the entered personal identification number is received at the server 12, e.g., using web service via the communications link 32 and the database 38 is queried to determine if the entered personal identification number or secret code 46 or fingerprint 47 matches the personal identification number 46 or password 47 in the database 38 for the customer's account 44. In various embodiments, in 226, a true or false value is returned from the server 12 to the point of sale device 28.

[0039] In various embodiments, in 228, a determination is made at the point of sale device 28 as to whether or not the customer code entered is valid and, if so, the method proceeds to 230 and, if not, the points are not allowed to be used.

[0040] In 230, in various embodiments, a request is sent from the point of sale device 28 to the server 12 to reduce credit points 44 in the customer's account by the number of credit points 44 used for the purchase. In various embodiments, in 234 the server 12 reduces the number of credit points used in the point of sale transaction from the customer's account 42 in the database 38.

[0041] In some embodiments, in 236, the server 12 returns, to the point of sale device 28, an indication as to whether the record for the customer has been successfully updated.

[0042] In some embodiments, in 238, a determination is made as to whether or not the credit points 44 were successfully deducted from the customer's account 42.

More particularly, in some embodiments, the point of sale device 28 obtains in 230 an indicator from the server 12 whether the credit points 44 were deducted successfully. In some embodiments, if a successful indicator is returned, the point of sale device 28 prints out a sales receipt for the customer and the process concludes. If unsuccessful, the sale transaction is voided and the process starts over, such as from 206.

[0043] FIG. 3 is a flowchart illustrating additional details for block 214 of FIG. 2, in accordance with various embodiments.

[0044] In some embodiments a customer initiates a sale transaction where the point of sale device accepts 302 or takes in a product code and quantity purchased.

[0045] In 304, for every sale transaction line being recorded, the total purchased amount will be accumulated, in the embodiments shown in FIG. 3, until after the last item to be purchased 306 is recorded. In some embodiments, if the accumulated credit points required has reached the customer's available credit points, the customer can pay using cash, credit, or other forms of payment in addition to or instead of credit points (see 218 in FIG. 2). In some embodiments, the process of accepting product code, quantity purchased and computing the accumulated credit points amount and cash amount is iterative until it is the last item to be purchased. With the accumulated computed credit points amount, customer can be informed by the cashier or sales staff of his insufficient available credit points if the total computed credit amount is more than the available credit points.

[0046] FIG. 4 is a flowchart illustrating additional details for block 220 of FIG. 2, in accordance with various embodiments.

[0047] In some embodiments, when a customer confirms to use his available credits for a purchase, the customer is required to enter his secret code or PIN 46 or fingerprint 47 in the point of sale device 28. This is mainly to validate that the customer is authorized to utilize credit points given by the organization or administrator, in some embodiments. The secret code is received in 402.

[0048] In some embodiments, the request 220 from the customer to deduct the available credit points must include the customer secret code 46 or fingerprint image 47. The secret code can be a PIN, date of birth, or other sort of secret code, in various embodiments. In 404, if the secret code or fingerprint image and the customer identifier do not match what is in the database 38, a false indicator will be returned in 412 to the point of sale device 28. In the embodiments shown in FIG. 4, the customer

is allowed to re-try 406 to enter the secret code or fingerprint. In the embodiments shown in FIG. 4, the number of re-tries is stored 408 in a logfile 410 (see FIGS. 1A and 1B) in the point of sale device 28, such as for an audit trail purpose. In some embodiments, the customer can use different types of secret codes 46. The number of tries or retries of each different type of secret code 46, e.g., PIN or date of birth, is stored separately in the logfile 410 (see FIGS. 1A and 1B) in some embodiments. If the secret code 46 and the customer identifier 40 match with that in the database 38, a true indicator is returned in 412 to the point of sale device 28. In response to the secret code 46 and the identifier 40 having been validated and approved, the available credit points can be deducted in 230 (see FIG. 2).

[0049] While some embodiments disclosed herein are implemented in software, alternative embodiments comprise hardware, such as hardware including digital logic circuitry. Still other embodiments are implemented in a combination of software and digital logic circuitry.

[0050] Various embodiments comprise a computer-usable or computer-readable medium, such as a hard drive, solid state memory, flash drive, floppy disk, CD (read-only or rewritable), DVD (read-only or rewritable), tape, optical disk, floptical disk, RAM, ROM (or any other non-transitory medium capable of storing program code) bearing computer program code which, when executed by a computer or processor, or distributed processing system, performs various of the functions described above.

[0051] Some embodiments provide a carrier wave or propagation signal, medium, or device embodying such computer program code for transfer of such code over a network or from one device to another.

[0052] In compliance with the patent laws, the subject matter disclosed herein has been described in language more or less specific as to structural and methodical features. However, the scope of protection sought is to be limited only by the following claims, given their broadest possible interpretations. The claims are not to be limited by the specific features shown and described, as the description above only discloses example embodiments.

CLAIMS

1. A server comprising:
 - a processor, memory, and a data bus, and configured to execute a multi-tasking, multi-user operating system supporting multiple simultaneous sessions;
 - a network adapter coupled to the processor and configured to receive a connection from a point of sale terminal; and
 - a database coupled to the processor and arranged to associate identification cards with respective electronic accounts for customers, the database including entries for customer identifiers, account codes for respective customers, amount of credit points in respective accounts, fingerprints and secret codes for respective accounts;
 - the server being configured to add credit points to one of the accounts on a periodic basis;
 - the server being configured to receive an inquiry as to the amount of credit points in the account of a first one of the customers from a first one of the point of sale terminals, the inquiry including customer information data, the server being configured to retrieve information representing the amount of credit points in the first cardholder's account from the database, and to send the amount of credit points in the first cardholder's account to the first point of sale terminal;
 - the server being configured to receive, from the first point of sale terminal, a request to validate the customer for conclusion for a sale transaction, the request including a customer identifier and at least one of a customer secret code and customer fingerprint, the server being configured to compare the secret code from the point of sale terminal to the secret code in the database associated with the customer identifier and, if there is a match, to validate the customer; and
 - the server being configured to receive, from the first point of sale terminal, a request to deduct credit points from the account of the validated customer, the request to deduct resulting from a purchase of items at the first point of sale terminal and the request to deduct including an amount of points based on the cost of the purchase items and information identifying the account of the validated customer.

2. A system in accordance with claim 1 and further comprising a dedicated line and a point of sale terminal in communication with the server via the dedicated line.

3. A system in accordance with claim 2 wherein the customer identifiers comprise National Registration Identity Card identifiers.

4. A system in accordance with claim 2 or 3 wherein the point of sale terminal is configured to read a card.

5. A system in accordance with claim 2 or 3 wherein the point of sale terminal is configured to read a customer identifier from a National Registration Identity Card.

6. A system in accordance with claim 2 or 3 wherein the point of sale terminal is configured to read a customer identifier from an employee card.

7. A system in accordance with claim 2 or 3 wherein the point of sale terminal is configured to inquire as to whether a customer would like to pay using a mix of cash and credit points.

8. A system in accordance with claim 2 or 3 wherein the point of sale terminal includes at least one of a keypad and fingerprint scanner and wherein a customer secret code is entered at the point of sale terminal using the keypad or a fingerprint is entered at the point of sale terminal using the fingerprint scanner.

9. A system in accordance with claim 2 or 3 and further comprising a firewall between the server and the point of sale terminal.

10. A method comprising:

- associating an identification card, issued from an organization to persons, with respective electronic accounts for at least some of those persons in a database in a server, the database including entries for the persons, accounts for respective of the persons, credit points in respective accounts, and personal identification numbers for respective accounts, the identification cards bearing data capable of being read by a point of sale device, the data identifying the persons holding the respective cards;
- periodically depositing credit points in the account of a first one of the persons by changing data in the database;
- receiving an inquiry as to the amount of credit points in the account of the first person from a point of sale device;
- retrieving information representing the amount of credit points in the first person's account from the database using a dedicated line between the point of sale device and the server;
- returning the amount of credit points in the first person's account to the point of sale device;
- determining, at the point of sale device, the amount of credit points required for a purchase of goods or services by the first person;
- determining if the amount of credit points in the first person's account is at least as much as the amount of credit points required and, if not, inquiring at the point of sale device as to whether the first person would like to pay using a mix of cash and credit points;
- requesting that the first person enter his personal identification number or fingerprint at the point of sale device and receiving a request, at the point of sale device, to deduct a number of credit points from the first person's account; and
- receiving the entered personal identification number or fingerprint, using the dedicated line, and querying the database, to determine if the entered personal identification number matches the personal identification number in the database for the first person's account and, if so, deducting the requested number of credit points from the first person's account in the database.

11. A method in accordance with claim 10 wherein if the entered personal identification number or fingerprint matches the personal identification number or fingerprint in the database for the first person's account, the point of sale device authorizes the purchase of goods or services.

12. A method in accordance with claim 10 wherein the organization that issues the cards is a governmental authority or employer.

13. A method in accordance with claim 10 wherein the organization that issues the cards is a national governmental authority and wherein the cards contain security features of national identification.

14. A method in accordance with claim 10, 11, 12, or 13 wherein the cards do not bear personal identification number data.

15. A method in accordance with claim 10 wherein inquiring at the point of sale device as to whether the first person would like to pay using a mix of cash and credit points comprises inquiring whether the first person would like to use all credit points in his accounts plus an amount of cash necessary to total the amount of credit points required for a purchase of goods or services by the first person.

16. A method in accordance with claim 10, 11, 12, or 13 wherein associating the identification cards with respective electronic accounts for persons in a database comprises providing electronic accounts for a predetermined subset of the people to whom cards have been issued.

17. A non-transitory computer readable medium bearing computer program code that, when executed in a computer causes the computer to:

define a database including entries for customer identifiers, account codes for respective customers, amount of credit points in respective accounts, fingerprints and secret codes for respective accounts;

receive an inquiry as to the amount of credit points in the account of a first customer from a point of sale terminal, the inquiry including customer information data;

retrieve information representing the amount of credit points in the first cardholder's account from the database;

send the amount of credit points in the first cardholder's account to the point of sale terminal;

receive, from the point of sale terminal, a request to validate the customer for conclusion for a sale transaction, the request including a customer identifier and a customer secret code or fingerprint;

compare the secret code or fingerprint from the point of sale terminal to the secret code or fingerprint in the database associated with the customer identifier and, if there is a match, validate the customer; and

receive, from the point of sale terminal, a request to deduct credit points from the account of the validated customer, the request to deduct resulting from a purchase of items at the point of sale terminal and the request to deduct including an amount of points based on the cost of the purchase items and information identifying the account of the validated customer.

18. A computer readable medium in accordance with claim 17 wherein the customer identifiers consist of at least one of National Registration Identity Card identifiers and employee numbers.

19. A computer readable medium in accordance with claim 17 wherein the secret codes comprise respective personal identification numbers.

20. A computer readable medium in accordance with claim 17, 18, or 19 and further configured to cause the computer to send a confirmation code associated with the purchase of items to the point of sale terminal in response to receiving the request to deduct credit points.