

- 1 -

“A Vending Machine and System”INTRODUCTION5 Field of the Invention

The invention relates to automatic vending machines.

Prior Art Discussion

10

It is known to provide a vending machine for vending printed documents for products such as mobile phone top-up and train tickets. However such machines lack versatility in the range of products sold, and many require considerable staff time.

15

US20030104802 describes a vending machine having a local database and a wireless interface to control servers.

20

The invention is therefore directed towards providing a vending machine and system for more versatile vending of products, particularly products which can be represented or take the form of data or codes having a value such as a parking permit or a mobile phone top-up.

SUMMARY OF THE INVENTION

25

According to the invention there is provided a vending machine system comprising:

30

a plurality of vending machines, each including a processor, a customer input interface, a receiver for receiving payments, a display screen, and at least one printer,

- 2 -

a central controller for communicating via a wide area network with the vending machine to transmit products in the form of product data to the machines for vending;

5 wherein each vending machine comprises a database of a plurality of different types of products and user interface structures for menu-driven selection of products;

10 each vending machine comprises a touch screen and the processor of each vending machine is programmed to use the navigation structure commands of the database to drive user interfacing limited to selection of displayed options; and

15 wherein each vending machine processor dynamically maintains a log of events and uploads the log to the central controller, and the central controller dynamically downloads products according to demand.

In one embodiment, the central controller comprises an interface for receiving products from a plurality of suppliers, said interface receiving the products in
20 encrypted format according to an encryption scheme of the supplier and re-encrypting the products according to an internal encryption scheme.

In one embodiment, the central controller dynamically instantiates an object from a supplier class upon receipt of products, populates the object attributes with
25 products, and decrypts the products using instructions of object methods.

In one embodiment, the central controller initially validates the received products by automatically comparing the structure of a file holding the products with a reference template.

30 In one embodiment, the central controller decrypts the products to a binary format without any user interface, and re-encrypts to the internal encryption protocol.

- 3 -

In another embodiment, the binary format is maintained for less than 10 seconds.

In one embodiment, each vending machine processor is programmed to establish contact with the central controller, but to only perform non-vending operations
5 according to instructions dynamically downloaded by the central controller.

In one embodiment, the central controller downloads instructions referring to functions stored on the vending machine database, and the vending machine processor activates said functions only upon receipt of the instructions from the
10 central controller.

In one embodiment, the central controller downloads a mark-up language security file with instructions and products to each vending machine, and each vending machine processor parses the mark-up language file to extract instructions for
15 processing the products.

In one embodiment, said extracted instructions refer to stored functions in a library of functions for processing products in a received security file.

20 In one embodiment, said instructions are SQL database functions for writing of the encrypted products to a database table.

In one embodiment, the machines and the controller communicate wirelessly, via a wireless network.
25

In one embodiment, the products are arranged in a structure comprising, from top down, a product definition, at least one supplier, and at least one product for each supplier.

30 In one embodiment, each machine further comprises an automatic reader such as a bar code scanner or an RFID reader, and the reader reads a code of an item presented by the customer to trigger a transaction in part or in full.

- 4 -

In one embodiment, the processor recognises codes read by the automatic reader, and uses the codes to direct input of a payment and upload of the payment to an external system.

- 5 In one embodiment, the controller controls the range of products for each machine so that it is suited to physical location of the machine.

In one embodiment, each machine has a security printer for printing a durable and/or a secure ticket as a product.

10

In one embodiment, each machine includes at least one dedicated advertising screen.

- 15 In one embodiment, the controller controls advertising content for each machine according to its location.

In one embodiment, each vending machine comprises a housing having means for wall-mounting and a removable modular pedestal.

20 DETAILED DESCRIPTION OF THE INVENTION

Brief Description of the Drawings

- 25 The invention will be more clearly understood from the following description of some embodiments thereof, given by way of example only with reference to the accompanying drawings in which:-

Fig. 1 is a diagram showing a vending machine system of the invention;

- 30 Fig. 2 is a block diagram of the architecture of a vending machine of the system;

Fig. 3 is a perspective view of a vending machine; and

- 5 -

Figs. 4 and 5 are diagrammatic front and side views showing the internal parts of the machine

5 Description of the Embodiments

Referring to Fig. 1 vending machines 1 are located at various retail premises such as a shop, a forecourt, or a hotel. The machines 1 communicate via a mobile network 2 with a network operations centre (NOC) 3 having databases 4. The NOC
10 3 in turn communicates via the network 2 with various product supplier systems 10. Also, the NOC 3 communicates via a firewall 11 and the Internet with remote systems for reporting and archiving purposes.

The commercial basis of operation of the machines 1 is that they convert cash to
15 credit, receiving money in cash or card form from customers and providing products in the form of data or codes having a value. The data or codes are in this embodiment printed however it is envisaged that they may alternatively be outputted electronically such as via Bluetooth to a mobile device. The range of products is extremely wide, and includes mobile phone top-up, international call
20 credit, mobile phone content (logos, ring tones, games, or text alerts), parking discs, refuse tags, redeemable vouchers, coupons, cinema or concert tickets, travel (bus or train) tickets, and advertising content, among others. They may alternatively be referred to as electronic or e-vending objects.

25 Referring to Figs. 2 to 5, each machine 1 comprises a PC processor (motherboard) 30 connected to:

a touch screen 32,
a note reader 33,
a coin mechanism 34,
30 a barcode scanner 35,
a conventional printer 36,
a security printer 37,
audio speakers 38, and

- 6 -

a database 40.

Physically, each vending machine 1 comprises a housing 20 which may be wall-mounted by screw fastening to a wall W, and/or may rest on a pedestal 21. The machine may additionally include a payment card reader, and/or a dedicated advertising screen.

Thus for data and instruction input the machine 1 has both the touch screen 32 and the bar code reader 35. The latter allows a range of very useful products including for example fine payment, in which the customer presents a fine notification for scanning, the reader 35 reads the bar code, and if necessary extracts the details using data either retrieved via the modem 31 in real time or previously downloaded offline and stored locally in the database 40, then makes the payment.

The devices 33, 34 and 35 allow versatility in how money is paid.

For output of a tangible docket for supplying products, the first printer 36 is used. However, the security printer 37 prints on paper with holograms for products such as gift vouchers. The printer 37 may print a range of different security items with hologram or other anti-counterfeit measures.

System Hardware

The Network Operations Centre (NOC) is a fully redundant system. It comprises two servers. Storage is RAID 5, with current storage at ½ a Terabyte. This can be easily expanded if necessary. Both servers have twin 2GHz CPU's, and 2 GB of RAM. Both servers are on a frequent backup schedule, which uses a high speed tape drive. The NOC 3 has a secure, permanent ADSL (Asynchronous Digital Subscriber Line) link. Communication to the vending machines is firewalled. This firewall includes full packet-level firewall facilities, in addition to the inherent NAT (Network Address Translation) security and port-blocking of other routers. It also provides protection from Dos/DDos (Denial of Service/Distributed Denial of Service) attacks and IP anti-spoofing. In the event of ADSL failure, the NOC has

- 7 -

dial up RAS support over GSM, so vending machines can dial the NOC directly and communications can continue.

NOC 3 Product Processing

5

When a product supplier allocates products (such as a mobile operator allocating PINs) for the machines 1 they must be communicated in a secure manner to avoid theft. Also, they must be distributed in an efficient manner across all of the machines 1 in the network with a ready supply at each machine at all times.

10

The processor 30 maintains the database 40 as a relational database, in which there are tables for the various products. The table fields are used by the processor 30 to drive an option selection-only navigation menu structure on the touch screen 32.

15 Because there is no keyboard or any other type of input device, the user is only permitted to select options on the touch screen in a particular restricted manner. Because the user can only navigate through specific navigation menus there is no opportunity to gain unauthorized access to the database.

The products are routed to the NOC 3 as follows:

- 20
- An encrypted email is transmitted by the product supplier to an email address of the NOC 3.
 - The NOC 3 performs an initial validation of the file by checking the structure of the file. If the validation fails the NOC 3 sends alert messages to configured addresses.

25

 - The NOC 3 identifies the source of the supplier according to the email source address.
 - The NOC 3 then verifies the IP address associated with the email as a known and valid address, as a security check.
 - The NOC 3 uses one of the tables in its database to retrieve an object oriented class associated with the relevant supplier.

30

 - It uses the class to instantiate an object for the file, by populating the attributes of the class with the product data in the file.

- 8 -

- The NOC's processor then uses executable code of the object's methods to decrypt the product data. The decryption is to an internal format. This format is in binary code with machine-only access, there being no user interface to the decoded data. Also, the NOC's processor immediately,
5 within seconds, re-encrypts the data to a protocol for the system.

Product Download

10 The NOC 3 dynamically determines appropriate times for downloading additional products to the machines 1, according to demand patterns. The following is a sequence for a download.

- Each vending machine 1 receives a batch of products for vending by the processor 30 hosting web services which are addressable by the NOC 3 via the mobile network.
- 15 - The machine 1 establishes communication with the NOC 3 by dialling via GSM, the machine 1 rejects the call. The machine initiates a GPRS connection and opens a secure HTTP connection with the NOC 3.
- The NOC 3 then generates an encrypted XML security file. This file includes the products, in this embodiment the encrypted PIN codes. This file
20 also includes executable code instructions to allow the processor 30 of the machine 1 to process the products in the file.
- Upon receipt of the file, the processor 30 parses the file and uses the data gleaned from the XML to retrieve functions comprising detailed instructions from a library for processing the products in the security file. These
25 instructions are mainly SQL statements for use in addressing the database 40. These instructions save the products to the database 40, while they are still encrypted.
- The processor 30 transmits, using an XML file, an acknowledgement to the NOC 3 to indicate safe receipt of the products.
- 30 - In real time, the processor 30 receives requests and payments for products and it dynamically decrypts the products one at a time to provide data for printing, such as a mobile phone top-up code, a ring-tone download code, or a parking ticket.

- 9 -

- At periodic intervals the processor 30 uploads log data tracking operation of the machine 1 to the NOC 3. This is performed as follows.

Centralised Control of Maintenance/Upgrade

5

The machines 1 are maintained at a data and software level by the NOC 3 in a manner controlled by the NOC 3. The sequence is as follows:

- The NOC 3 determines from a configured schedule that a particular machine 1 is due for maintenance/upgrade. It establishes a dial-up connection with the machine 1. The machine 1 detects that it has been dialled by the NOC's number and breaks the connection. This is effectively a poll by the NOC to trigger a maintenance routine.
- The processor 30 then connects to the NOC 3 by GPRS and activates a web service hosted by the NOC3. During this session the NOC 3 downloads the maintenance instructions.
- The processor 30 uses these instructions to perform the maintenance operations. These instructions can be for a wide variety of operations such as software upgrade, updates to the touch screen navigation structure to incorporate new products.
- During this GPRS session the Processor may also upload event log table contents to the NOC 3, so that the NOC 3 may track all activity. This is very important for commercial transactions.

25 The client machines can also send alerts to the NOC 3 via SMS. This is used to communicate out-of-service conditions back to the NOC 3 such as printers out of paper and note reader jammed. Upon receipt of an alert the NOC 3 will distribute the alert via email to any users subscribed to that alert.

30 The NOC will initiate communications with machines and then monitor to ensure that a machine does communicate. If a machine hasn't communicated within a defined time period the NOC will again initiate communications and again monitor for a response. After a set number of retries the NOC will send out an alert to indicate that a machine is not responding.

- 10 -

- The NOC continuously monitors for incoming SMS messages. When a message is received, the NOC will categorise the message according to application request. Once the request has been dealt with the NOC will send back a response to the
- 5 originator of the SMS. The NOC will monitor for delivery reports for any SMS messages it sends and upon receipt of a delivery report or failed delivery report will update the original SMS status to accurately reflect if a message reached its intended destination or not.
- 10 The NOC uses a combination of database triggers and file monitoring events to ensure that data held on the machines 1 matches the data held on the NOC. For example if a price change is applied to a product on the NOC, the NOC will automatically create a queued work item in the scheduling system. The work item contains the necessary information to update the relevant data on the machines 1.
- 15 The work item can be scheduled to run immediately or at any time in the future, allowing the system to manage the update of product data in a highly controlled manner.

Encryption/ Data Integrity

- 20 Communications between the NOC 3 and machines 1 is performed using 128 bit SSL encryption. When a machine 1 is commissioned, a unique X509 certificate is issued to it. This certificate is used as a security token in all communications with the NOC 3 so that the authenticity of the client machine can be verified. All
- 25 communications also use a user security token which must match a valid user on the NOC in order for communications to proceed.

- The NOC uses a combination of techniques to ensure data integrity within its systems. Foreign keys, primary keys and unique index constraints are used to
- 30 ensure that data duplication is avoided. These constraints for example are used to ensure that the same PIN cannot be created twice or the same PIN assigned to more than one machine 1.

- 11 -

The NOC uses triggers and foreign key constraints to disallow deletion of critical data. All data modifications performed on the NOC are fully audit trailed ensuring full traceability. The NOC has an alerting subsystem that it utilises to communicate information to subscribed users. The NOC uses this system to send notifications
5 when unexpected events occur or when the NOC's automated systems cannot resolve an issue or when the NOC needs to alert someone that it has processed a particular task such as generating invoices.

The alerting subsystem allows users to choose which notifications they wish to
10 receive ensuring that alerts are sent to relevant users.

The NOC 3 has a fixed Internet Protocol (IP) address, assigned by the Internet Service Provider (ISP). As the remote machine 1 addresses are dynamically assigned, via the GPRS network, the NOC 3 cannot connect to them, because they
15 don't have a fixed IP address. Instead they must connect back to the NOC over the GPRS network. They can either initiate the session themselves, e.g. if they run low on PIN stock, or the NOC 3 can trigger them to connect back if it needs to push updates to them. This works as follows:

20 If the remote machine 1 is dialed by anyone, the call is rejected and a HTTP session is initiated by the remote machine 1. The remote machine 1 can then login in to the NOC, and communication begins. This also allows service personnel to whom the machine number is known to trigger a NOC callback from the remote machine 1.

25 Link management and content communications between the NOC and the remote machine 1 is via encrypted XML, with different encryption keys used for both directions.

30 The NOC 3 is also capable of giving a full topology view of the network. This can be both nationally and internationally.

- 12 -

PIN Handler, Allocation, Tear-down, Reallocation

A "PIN handler" software function assigns PIN numbers to electronic products that suppliers cannot provide PIN numbers for. This identifies the product the customer
5 has chosen and also manages the product from a vending perspective. The PIN handler function is used for other mobile products such as ringtones, "wallpapers", alerts, and images. It could also apply for other cash collection products.

Taking the example of a game which has a product code of '1000'. This identifies
10 the game on a game supplier database. Multiple copies of this product code are to be sold. Several PIN numbers (15 digit number) are generated and assigned to this particular product. These PIN numbers are then sent to the remote machine 1. When the customer chooses the game with product code 1000, the remote machine 1 looks up the next available PIN for this product and accordingly prints this on the
15 vended ticket.

The customer then sends this number to the NOC 3 using SMS. The NOC 3 knows that this number is uniquely associated with product 1000 and initiates a download procedure from the games supplier. If the customer texts an invalid number, no
20 download procedure is initiated. If the particular PIN number has already been used, no download occurs. The PIN is a unique number and can only be used for a single download process. Thereafter, it is discarded and is not available for immediate use again.

25 When a number has been used, it is quarantined for a defined period of time and can be reallocated to a particular product.

PIN numbers stored in the 'PIN pool' in the NOC 3 are assigned a status. This indicates whether the PIN is available for (a) sending to a machine, (b) already has
30 been sent to a machine, (c) has been pulled back from a machine or (d) has been sold. As part of security measures to prevent fraudulent attempts to download games by customers guessing PIN numbers, only PIN numbers sent to machines are checked. This allows a large pool of numbers to be available for download.

- 13 -

PIN numbers have tangible commercial value. For example for mobile/phone top-ups the PIN numbers are worth their top up value. Once this data is visible, there is a risk that it may be misappropriated. There are several stages at which the PIN number may be compromised, such as:

- while stored in the NOC 3,
- while being sent to a machine 1, or
- while stored in the machine 1.

PIN numbers are supplied to the NOC 3 in encrypted format, using PGP. PGP uses two keys, one public, one private. The NOC 3 public key is used by suppliers, to encrypt the PINs they send to the NOC 3. Once encrypted, this data can only be decrypted with the private key. This ensures that if the email is incorrectly addressed or intercepted by some means, the unintended recipient cannot view the data.

Once the PINs are required by the NOC 3, they are imported into a repository by a PinManager function. The PinManager takes the PGP encrypted file and decrypts it using the private key. Once the file is decrypted, the individual PINs are immediately encrypted again, using 128 bit encryption and are then transferred to NOC 3 PIN repository. The decryption, re-encryption and storing happens automatically, with no user intervention. At no stage of this process are the PINs visible to any staff managing the NOC 3.

The need may arise to verify if a PIN is valid. For instance a customer may call and state that their PIN doesn't work. There is then a need to validate that their PIN belongs to a NOC 3 pool. A function PINValidator allows help desk operators to validate PIN numbers. The PINValidator asks the helpdesk operator to enter the customers serial number, associated with the PIN, and then returns either a valid, or invalid response.

- 14 -

Filter Handling (Throttling) - Logical Drill Down

Products are defined as various levels in the remote machine 1. They are presented via a plasma touch screen with associated icons for each product. A main menu lists the type of products available, i.e. top-up, call card, games, tones and parking. These are at the product definition level. Each product definition has suppliers. Each supplier can have sub-suppliers, and ultimately each supplier or sub supplier supplies product, which is what the customer purchases. For Top Up the hierarchy is simple:

10	L1: Product Definition:	Top Up	
	L2: Product suppliers:	Operator A; Operator B; Operator C	
	L3: Products:	Operator A	€5
		Operator A	€10
		Operator B	€5
15		Operator B	€10
		Operator C	€10

It is important to identify the handset so that the correct product is ordered. If a game is only written for make/model of handset, the customer cannot be allowed to order it for a different type of handset. The machine 1 therefore enables the customer to select their mobile type and the machine then displays the games available for this particular mobile type. This is where the supplier- sub-supplier relationship is used. For example A is a supplier, B is a supplier. Each handset is also defined as a sub supplier to the manufacturer supplier. This supplier – sub supplier relationship can have many loops, for example:

	L1: Product definition:	Mobile gaming
	L2: Product suppliers:	Manufacturer A
		Manufacturer B
		Manufacturer C
30	L2b: Sub suppliers:	Mobile (i)
		Mobile (ii)
		Mobile (iii)

- 15 -

L3: Products: Solitaire for Mobile (i) (product code 1000)
 Solitaire for Mobile (ii) (product code 1001)
 Solitaire for Mobile (iii) (product code 1002)

- 5 Each product's PIN number will then be used by the NOC 3 to identify the product code needed to initiate the download procedure. Each machine 1 has the ability to accept payment for and facilitate content delivery to mobile phones. A mobile content manager (MCM) of the NOC 3 breaks this process down into several steps.
- Import supplier product information for games, ring tones, logos, are written
 10 into an NOC repository
 - Define products and sale items.
 - Assign internal PIN numbers to these products.
 - Distribute these products and PINs to the relevant machines 1. When the customer buys the product, the PIN is printed on the ticket.
 - 15 - The customer texts the PIN back to NOC 3, which verifies that the PIN is valid.
 - The NOC 3 then requests a download URL for the customer's product from the relevant supplier.
 - The NOC 3 then pushes the URL, along with some marketing text, to the
 20 customer's mobile phone as a service message.
 - The user then clicks on the link contained in this message and the product then downloads to the phone.

25 The product information is imported from the supplier's content management system. This information can be in various forms such as excel, html, xml etc. A download may include: Supplier product ID; Product Name; Product images / animations / audio; and Product descriptions.

30 There is an import template for each supplier, so that the import of their data is seamless and maps directly into the NOC database. As part of the import process, the template generates alerts to any new products or updates. It can disable or enable entire product ranges at this stage, so that the NOC 3 may have the product data in the database, but it may not be for sale.

- 16 -

For PIN number generation and assignment the MCM validates the sale and consequently allows sale of a product at any price. It is not restricted to the fixed pricing of mobile short codes. It generates 15 digit PIN codes for each sale item.

- 5 These are randomly generated, unique codes. It then encrypts these numbers and stores them into the NOC repository.

- Depending on individual machine 1 configuration the appropriate products and their relevant PINs are transmitted, encrypted, to the machines 1. The customer
10 uses the simple drill down navigation system to get to the product they want, view the product details and make the appropriate payment. Once payment is made, the PIN is decrypted and printed on the customer's ticket. Also printed on this ticket are detailed instructions specific to their handset, on how to redeem their product. They are instructed to SMS the PIN number to a mobile number. This mobile
15 number is monitored by our PIN Handler.

- Once the SMS arrives at the PIN Handler, it is checked for validity. It checks if it exists in the repository (if it is a valid number) and if it has been sent to a machine 1. If both checks pass, then it looks up the sale item and formats a message to send
20 to the supplier to request the download URL.

- Once the download request message is formatted, according to the supplier's protocol, it issues a http post / get. If all is in order, the supplier replies with a download URL. This URL is used by the end customer to download their product.
25 This URL points to a page on the supplier's web server. Once it receives the URL from the supplier, it formats a message to be sent to the customer. This message thanks them for their purchase, and instructs them to go to the URL to download their product. This message is sent as a service SMS, so it can include the URL and it can be easily accessed by the user. Also included on the ticket are instructions on
30 how to download the product. Once the user goes to the link, they enter the supplier's content supply interface, and follow whatever instructions are supplied to download their product.

- 17 -

The whole process from the customer sending the PIN, to them receiving their download link, takes a few seconds, depending on network traffic.

Bar Code Reader 35

5

This is used to gather information from the customer as they undertake a transaction. The machine 1 allows the facility to make a payment against a product (goods or service), for example, local authority standing charges. In this example the authority will send out a payment reminder to the householder. This reminder
10 will have an account number for the householder. This account number will also be in a barcode format.

The customer wishing to make a payment therefore brings this reminder notice with them. They drill down to the make payment screen for the appropriate authority /
15 product, i.e. >> Waterford city council >>standing charge. They are then prompted to scan in their bar code to identify themselves, and then select the amount they wish to pay. They insert the appropriate amount and a receipt is printed, indicating that payment of 'X' euro has been made to account 'Y' for product 'Z'.

20 This payment is then logged as a sale, except there is no PIN number required for it. Notification is then sent to the supplier (local authority) that the payment of X was made to account 'Y' for product 'Z'. Payment in this manner may be a part payment or payment in full against an account.

25 By using the bar code scanner to read in customer details and make a payment the machine 1 is used as a cash collection device.

The touch screen can display has a virtual keyboard under processor 30 instructions to also take in certain data in a similar fashion to that described above.
30 This will also include the ability to select part or full payments.

- 18 -

Advertising

The machine 1 displays additional advertising information on the touch screen 32 and in some embodiments also on an additional display in reasonable proximity to the machine 1. There can be any number of additional displays, each capable of displaying its own information stream. The displays can show static images or animated / moving pictures. The content to display is controlled by the NOC 3. Each machine 1 has a configuration file that enables the NOC 3 to send different content to different machines. The machine 1 loops through all of the advertisements on a timed basis, so that each advert can be shown for a different period of time. The NOC 3 also downloads the files to display to the remote machine 1.

The machine 1 runs on a single loop. When the machine application starts, it opens the advertising table from the remote database. It reads the first entry, which contains the filename to display and the duration of the advert. It then loads the filename and displays it on the relevant screen. When the advertisement time has expired, it goes to the next record and loads and displays that advert for the correct period of time. When it reaches the last advert, it goes back to the start again and continues displaying the relevant adverts / files.

To stop showing an advert, the NOC 3 can simply disable the advert in the machine 1. By toggling the enable field in the advert table, the advert can be turned on and off dynamically. There is no need to visit the machine to manually change the adverts. New adverts are downloaded as and when required. There is also the facility to remotely delete adverts no longer in use to conserve hard disk storage.

Product Call Down / Draw Down Procedure

The machines 1 can operate with a PIN stock stored locally or in the NOC 3. The PIN stock is normally stored in the machine 1. This allows the machine to print tickets or receipts quickly using its own allocated local stock. This method results in each machine having stock, which may have an associated cost. An alternative is

- 19 -

to have the machine 1 carry no stock and have it draw down stock from the NOC 3 when required. This results in the NOC 3 containing all stock, so that it is shared between machines.

5 Virtual Stock Management System

The machines 1 operate with their own stock management system. For each product, the level of stock the machine will hold can be configured. There is a defined top-up level and a minimum stock level. When the machine is restocked,
10 each product is stocked to top-up level. As each PIN is sold, the stock level drops and when the stock level reaches the minimum stock level, the machine automatically contacts the NOC 3 and downloads enough stock to bring the stock level back to the top-up level. Master stock levels are dynamically maintained and controlled by the NOC 3. These levels are configurable on the NOC 3 per machine,
15 so that we can tailor the levels to suit the particular location requirements

NOC Controller Diagnostics

The NOC 3 performs efficient remote management of the network of machines 1. It
20 monitors, detects, modifies, fixes and logs any changes to the network. Some tasks include Topology view, Alarm mapping, Command trace facility, transaction logging, Communication active/live/failure/retrieval test, and Connectivity pulse testing.

25 Configurable GUI (Dynamic ICON allocation)

Each display on the touch screen 32 is built dynamically by the processor 30. Each button, for example, has a picture and text. The filename for the picture is stored in a database and the text to display is stored also. This allows the NOC to change the
30 screens dynamically according to configurations. This allows different products for display in different areas, for instance local authority parking discs. One can define parking for Waterford @ €1 per hour as a product and parking for Dublin @ €2 per hour as a product.

- 20 -

Additional products can be brought on line automatically. Upon commencement of a new supplier, the products are defined, the product data is downloaded, images and descriptions are downloaded to the remote machine 1, and the display automatically refreshes to include the new product. Thus, all machines are updated immediately nationwide and internationally as required.

Real Time Reporting

As the NOC 3 is in constant real time communication with all of the machines 1, the system continuously updates statistics for all products across all machines. With this information detailed sales information can be generated immediately and summary data can be given to the retailer and the machine at any predefined time interval, such as 12 hours, daily, weekly or monthly. Accountability and accuracy of data in real time is achieved. Different reporting, graphs, statistics and trends can be extrapolated from the data at a machine level, regional (cluster) level, national level or at the overall NOC level.

Vouchers and Gifts

One printer uses plain paper stock and is used for printing dockets. This paper is very thin and only intended to be used once, for example to use a PIN number and discard. The second printer is used for printing tickets. Tickets are printed on different media to the receipt printer. It uses much more durable thicker paper / plastic (weather proof) and is designed for more manual handling. They also incorporate anti counterfeit measures, in this embodiment holograms, a logo, and a barcode. For example, a parking disc needs to be verified visually by a parking attendant, so there must be some way of inspecting the ticket with the naked eye to ensure that it is not a counterfeit.

The invention is not limited to the embodiments described but may be varied in construction and detail.

Claims

1. A vending machine system comprising:
 - 5 a plurality of vending machines, each including a processor, a customer input interface, a receiver for receiving payments, a display screen, and at least one printer,
 - 10 a central controller for communicating via a wide area network with the vending machine to transmit products in the form of product data to the machines for vending;
 - 15 wherein each vending machine comprises a database of a plurality of different types of products and user interface structures for menu-driven selection of products;
 - 20 each vending machine comprises a touch screen and the processor of each vending machine is programmed to use the navigation structure commands of the database to drive user interfacing limited to selection of displayed options; and
 - 25 wherein each vending machine processor dynamically maintains a log of events and uploads the log to the central controller, and the central controller dynamically downloads products according to demand.
2. A vending machine system as claimed in claim 1, wherein the central controller comprises an interface for receiving products from a plurality of suppliers, said interface receiving the products in encrypted format according to an encryption scheme of the supplier and re-encrypting the
30 products according to an internal encryption scheme.
3. A vending machine system as claimed in claim 2, wherein the central controller dynamically instantiates an object from a supplier class upon

- 22 -

receipt of products, populates the object attributes with products, and decrypts the products using instructions of object methods.

4. A vending machine system as claimed in claim 3, wherein the central controller initially validates the received products by automatically comparing the structure of a file holding the products with a reference template.
5. A vending machine system as claimed in claims 3 or 4, wherein the central controller decrypts the products to a binary format without any user interface, and re-encrypts to the internal encryption protocol.
6. A vending machine system as claimed in claim 5, wherein the binary format is maintained for less than 10 seconds.
7. A vending machine system as claimed in any preceding claim, wherein each vending machine processor is programmed to establish contact with the central controller, but to only perform non-vending operations according to instructions dynamically downloaded by the central controller.
8. A vending machine system as claimed in claim 7, wherein the central controller downloads instructions referring to functions stored on the vending machine database, and the vending machine processor activates said functions only upon receipt of the instructions from the central controller.
9. A vending machine system as claimed in any preceding claim, wherein the central controller downloads a mark-up language security file with instructions and products to each vending machine, and each vending machine processor parses the mark-up language file to extract instructions for processing the products.

- 23 -

10. A vending machine system as claimed in claim 9, wherein said extracted instructions refer to stored functions in a library of functions for processing products in a received security file.
- 5 11. A vending machine system as claimed in claim 10, wherein said instructions are structured query language database functions for writing of the encrypted products to a database table.
- 10 12. A vending machine system as claimed in any preceding claim, wherein the machines and the controller communicate wirelessly, via a wireless network.
- 15 13. A vending machine system as claimed in any preceding claim, wherein the products are arranged in a structure comprising from top down, a product definition, at least one supplier, and at least one product for each supplier.
- 20 14. A vending machine system as claimed in any preceding claim, wherein each machine further comprises an automatic reader such as a bar code scanner or an RFID reader, and the reader reads a code of an item presented by the customer to trigger a transaction in part or in full.
- 25 15. A vending machine system as claimed in claim 14, wherein the processor recognises codes read by the automatic reader, and uses the codes to direct input of a payment and upload of the payment to an external system.
16. A vending machine system as claimed in any preceding claim, wherein the controller controls the range of products for each machine so that it is suited to physical location of the machine.
- 30 17. A vending machine system as claimed in any preceding claim, wherein each machine has a security printer for printing a durable and/or a secure ticket as a product.

- 24 -

18. A vending machine system as claimed in any preceding claim, wherein each machine includes at least one dedicated advertising screen.

19. A vending machine system as claimed in claim 18, wherein the controller
5 controls advertising content for each machine according to its location.

20. A vending machine system as claimed in any preceding claim, wherein each vending machine comprises a housing having means for wall-mounting and a removable modular pedestal.

10