US 20110106681A1

(19) **United States**

(12) **Patent Application Publication**

(10) **Pub. No.: US 2011/0106681 A1**

(43) **Pub. Date: May 5, 2011**

Cockerell et al.

(54) **ENTITY MANAGEMENT METHOD AND SYSTEM USING WIRELESS DEVICES**

(75) Inventors: **Alexander Cockerell**, Hampshire (GB); **Kevin Smith**, Wilton, CT (US); **Timothy Edward Plumridge**, Hampshire (GB)

(73) Assignee: **De La Rue International Limited**, Hampshire (GB)

(21) Appl. No.: **12/735,177**

(22) PCT Filed: **Dec. 19, 2008**

(86) PCT No.: **PCT/GB2008/004236**

§ 371 (c)(1), (2), (4) Date: **Jan. 13, 2011**

(30) **Foreign Application Priority Data**

Dec. 21, 2007 (GB) PCT/GB2007/004952

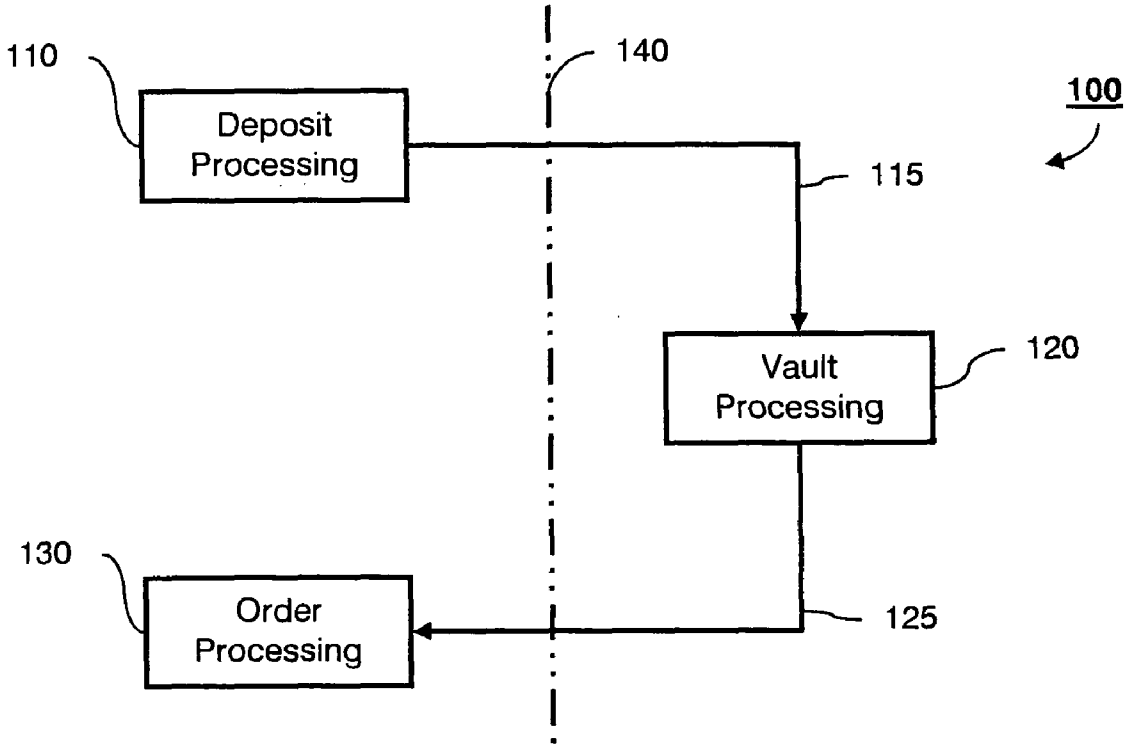
Publication Classification

(51) **Int. Cl.**
G06Q 40/00 (2006.01)
G06Q 10/00 (2006.01)

(52) **U.S. Cl.** **705/35**

(57) **ABSTRACT**

A method of providing information about a plurality of entities within a cash processing centre, the method comprising coupling a first entity with a first wireless device, coupling a second entity with a second wireless device, reading data associated with both the first and second wireless devices, pairing data associated with both the first and second wireless devices and retrieving information concerning the relationship between the first entity and the second entity based on the pairing. The entities are typically objects within the centre and the wireless devices are transmitters and/or receivers.



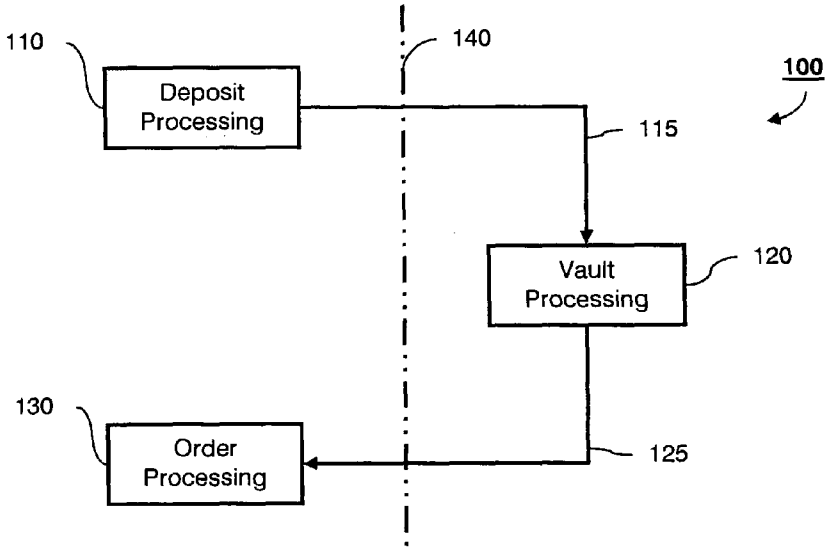


Figure 1A

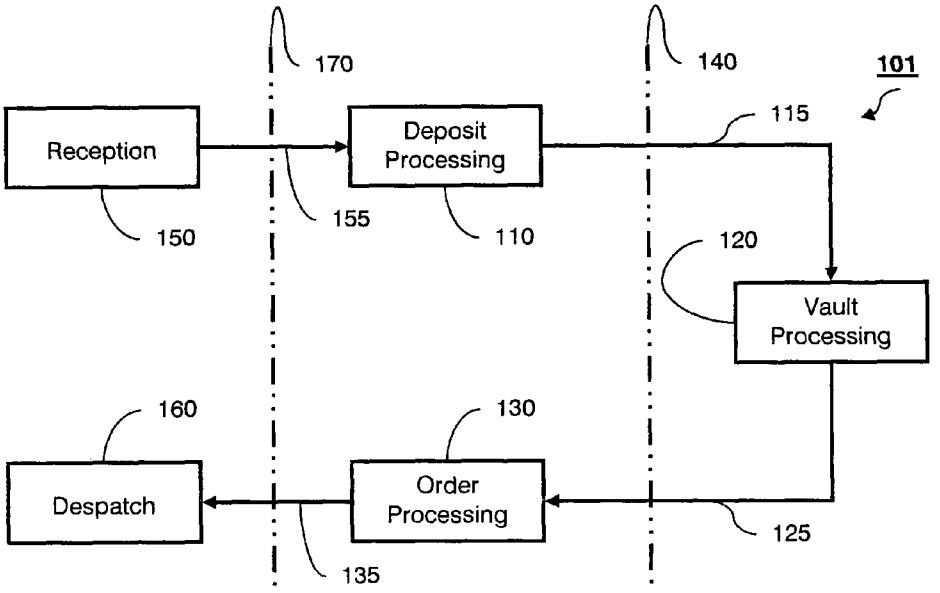


Figure 1B

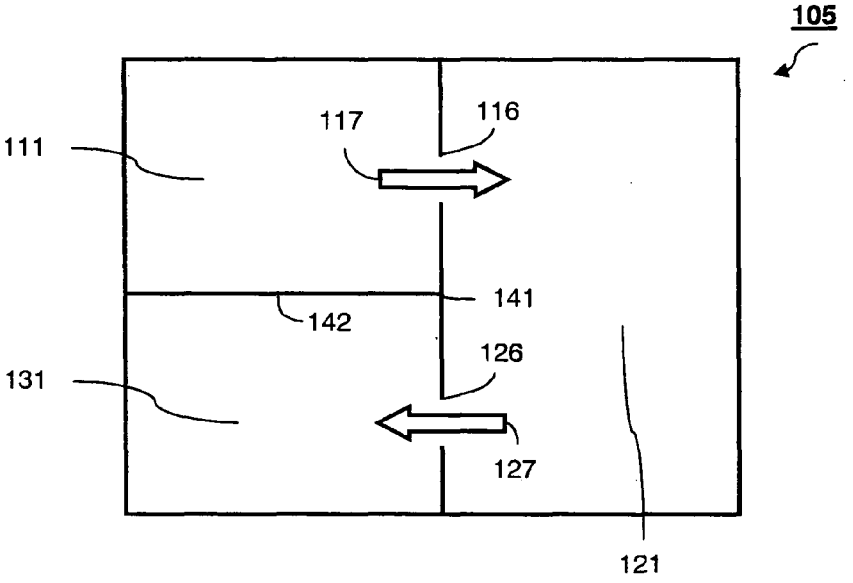


Figure 1C

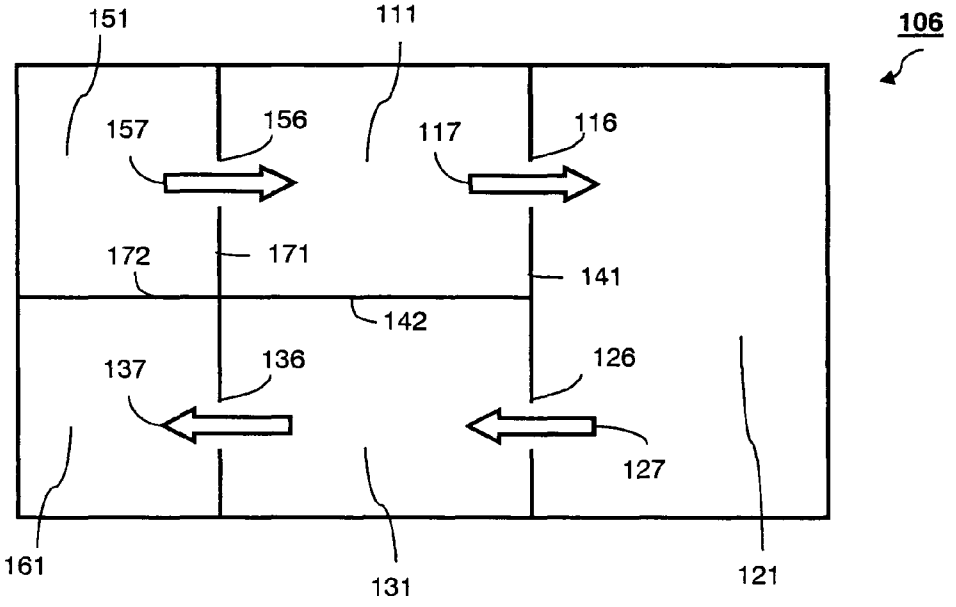


Figure 1D

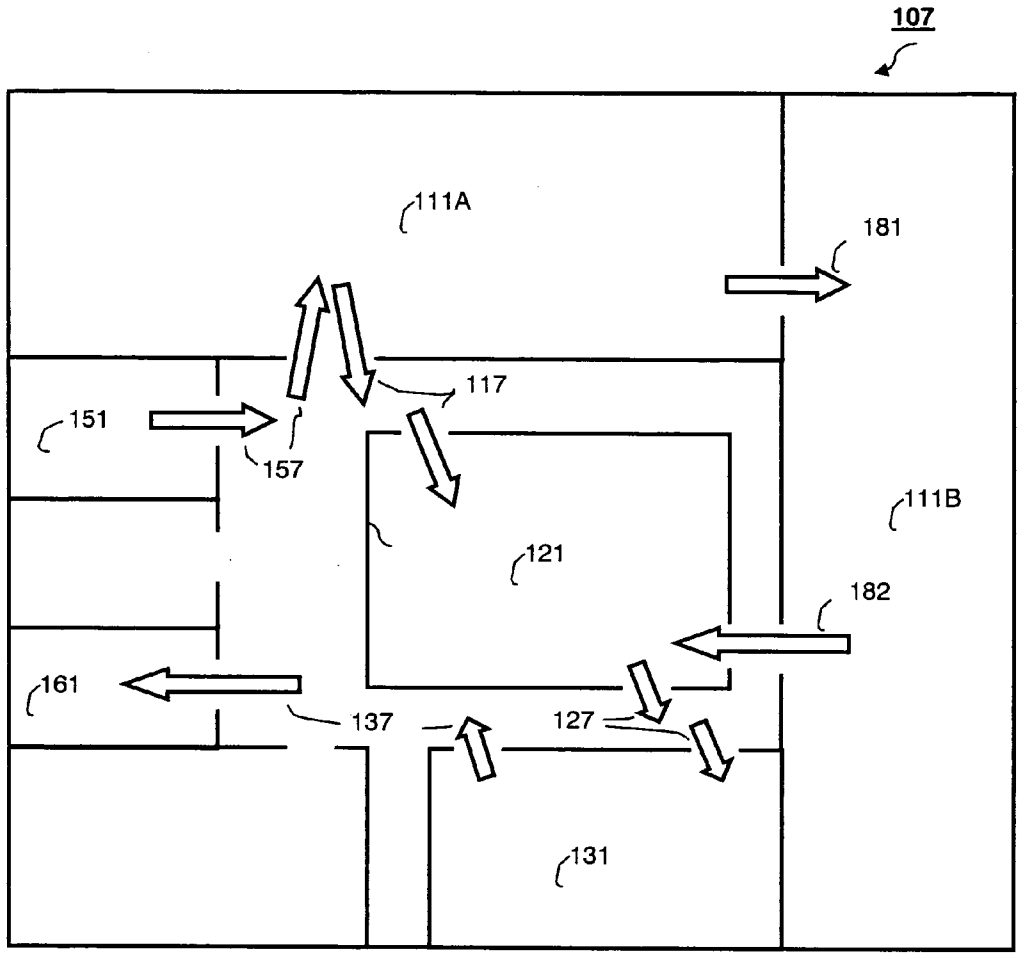


Figure 1E

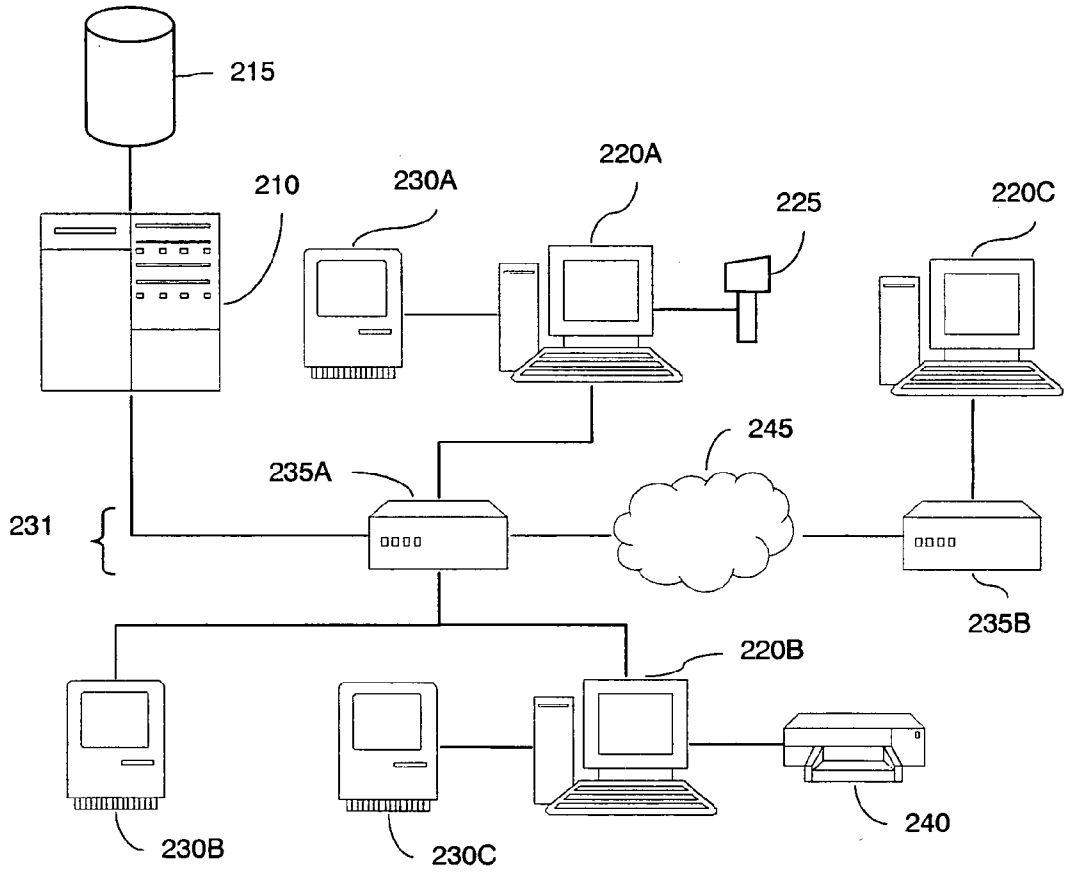

215
210
230A
220A
225
220C
245
235A
231
235B
220B
230B
230C
240

Figure 2A

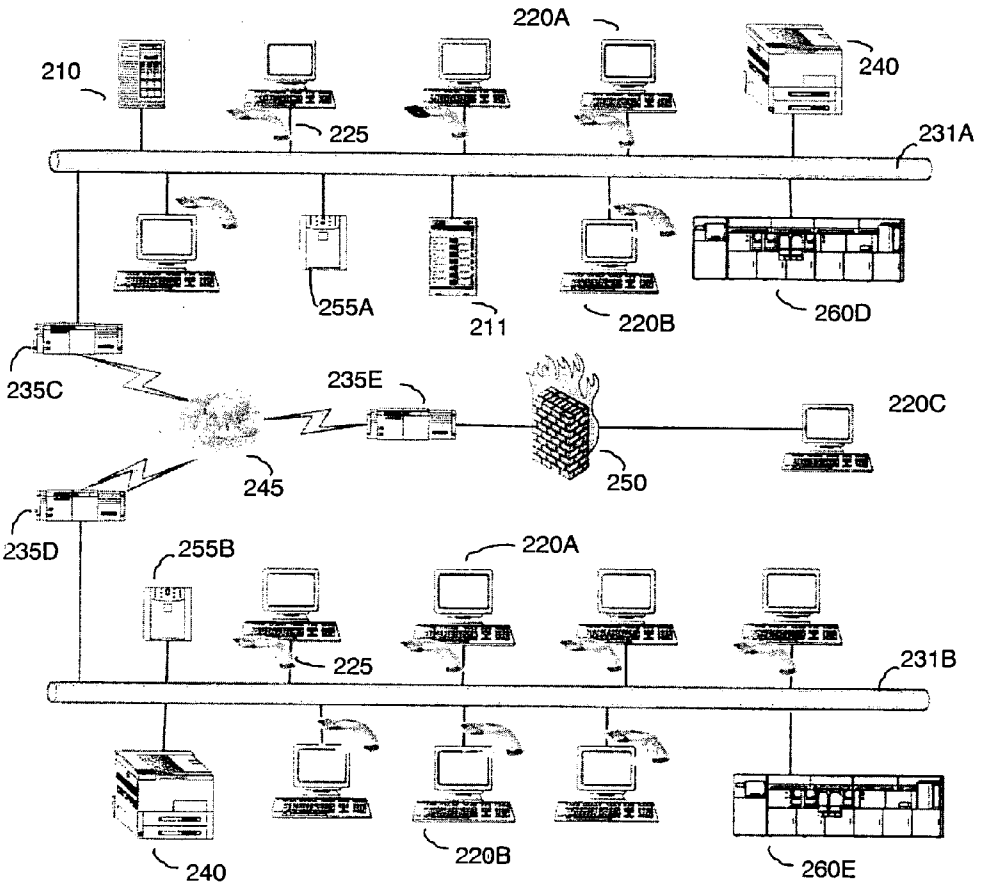

220A
210
240
225
231A
255A
211
220B
260D
235C
235E
220C
245
250
235D
255B
220A
225
231B
240
220B
260E

Figure 2B

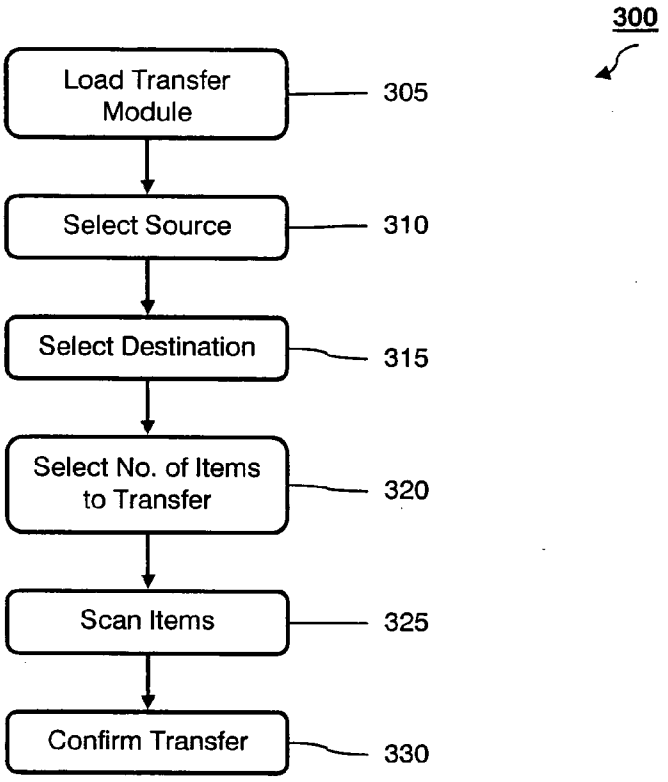


Figure 3A

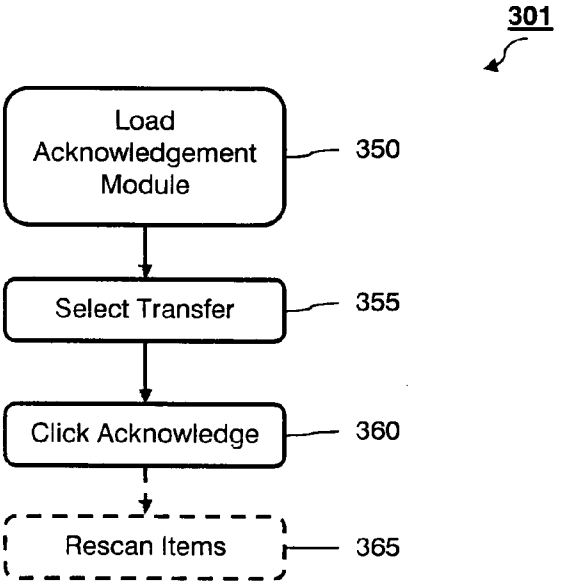


Figure 3B

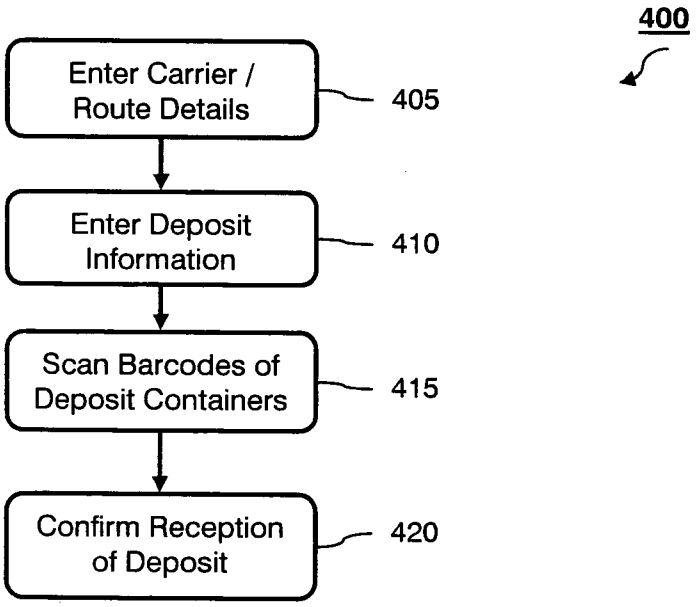

400
Enter Carrier / Route Details
405
Enter Deposit Information
410
Scan Barcodes of Deposit Containers
415
Confirm Reception of Deposit
420

Figure 4

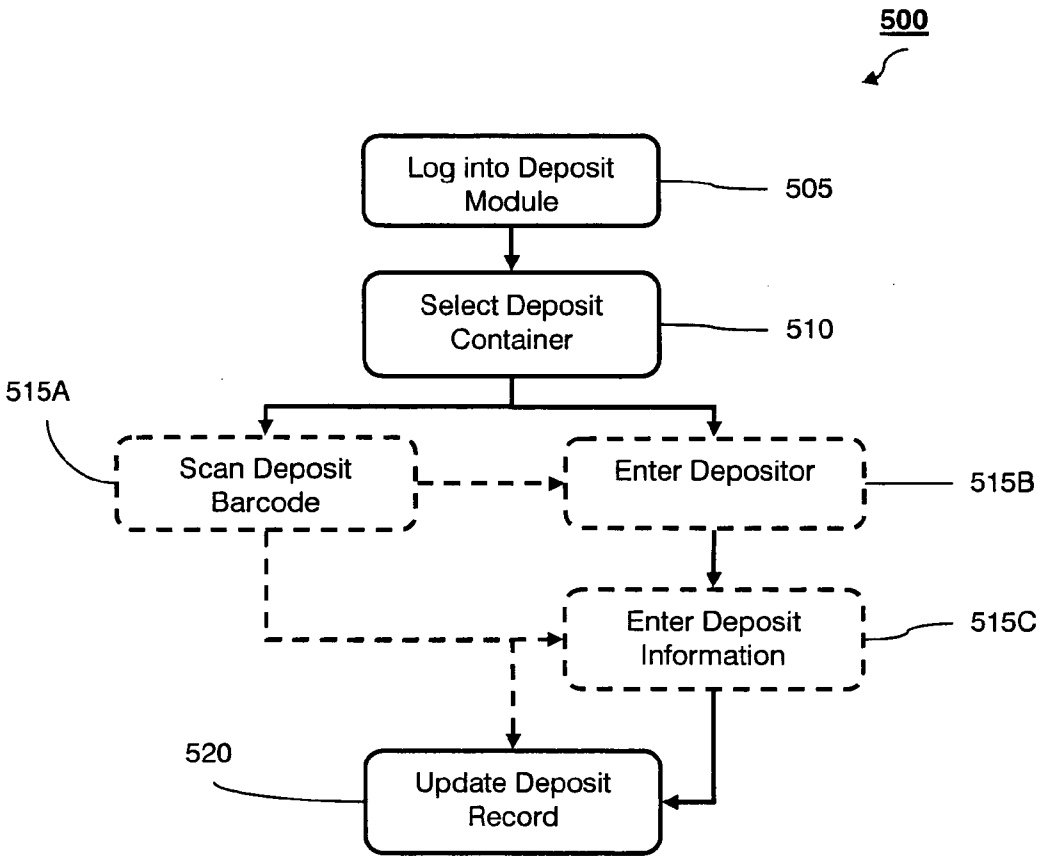

500
Log into Deposit Module
505
Select Deposit Container
510
515A
Scan Deposit Barcode
Enter Depositor
515B
Enter Deposit Information
515C
520
Update Deposit Record

Figure 5A

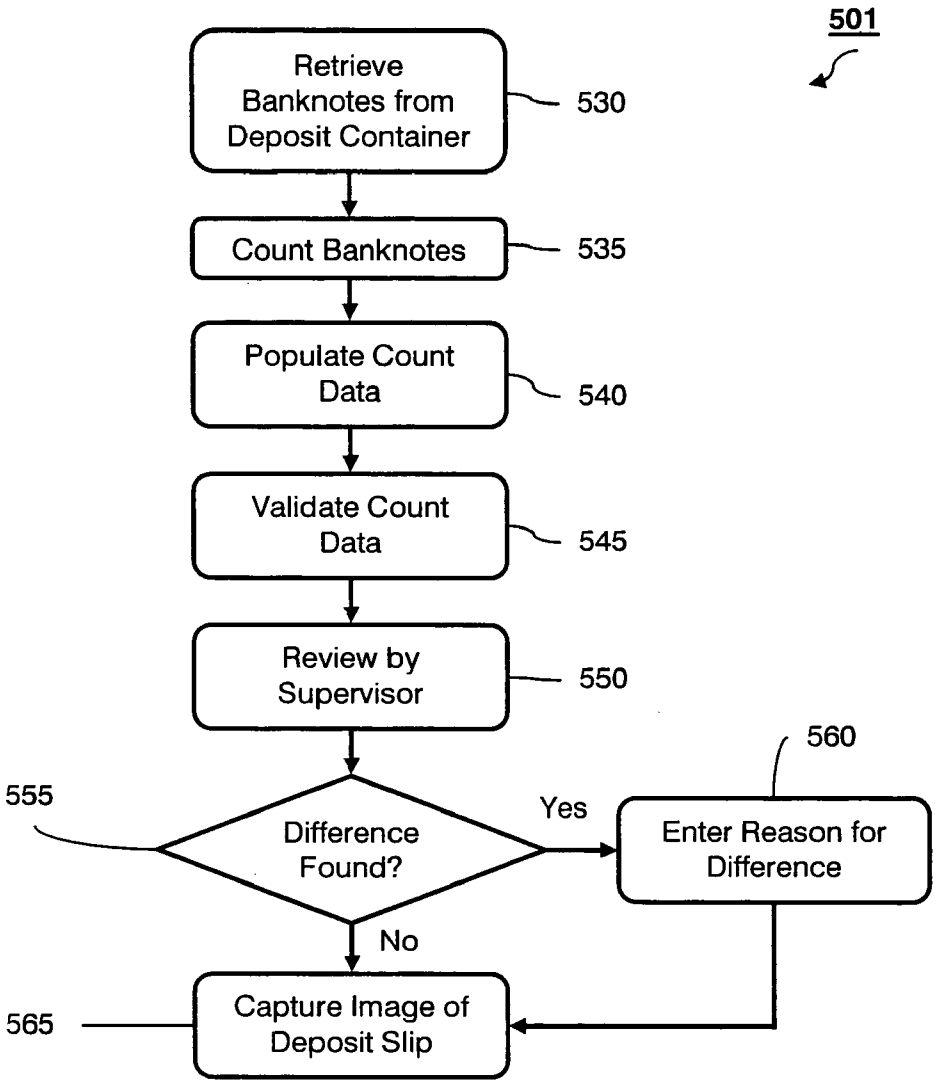

501
Retrieve Banknotes from Deposit Container
530
Count Banknotes
535
Populate Count Data
540
Validate Count Data
545
Review by Supervisor
550
555
Difference Found?
Yes
560
Enter Reason for Difference
No
565
Capture Image of Deposit Slip

Figure 5B

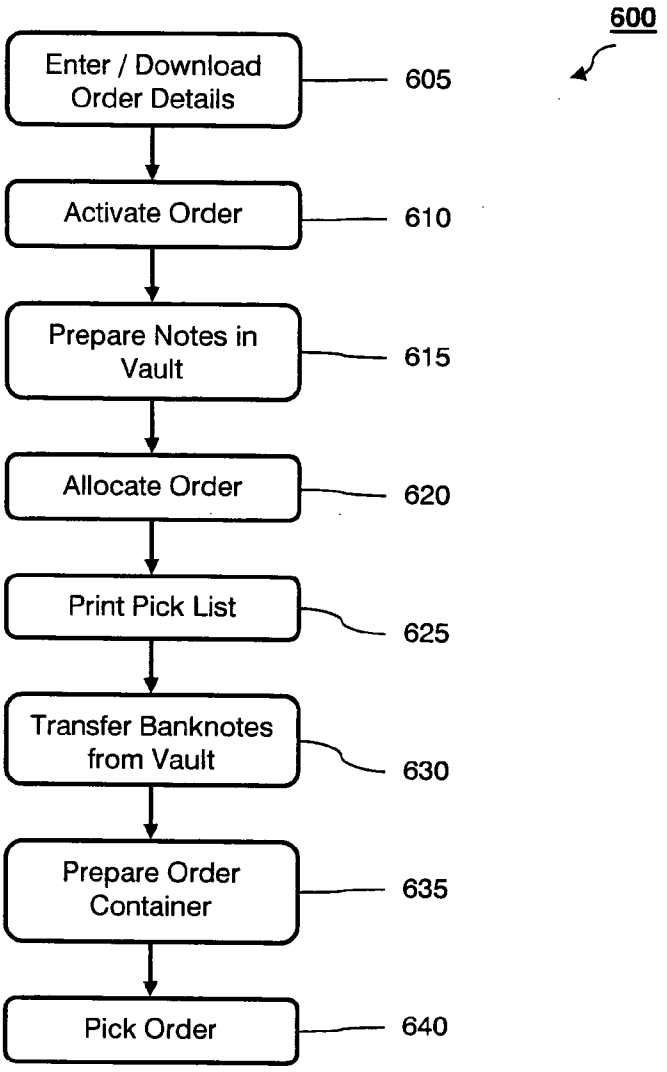

600
Enter / Download Order Details
605
Activate Order
610
Prepare Notes in Vault
615
Allocate Order
620
Print Pick List
625
Transfer Banknotes from Vault
630
Prepare Order Container
635
Pick Order
640

Figure 6

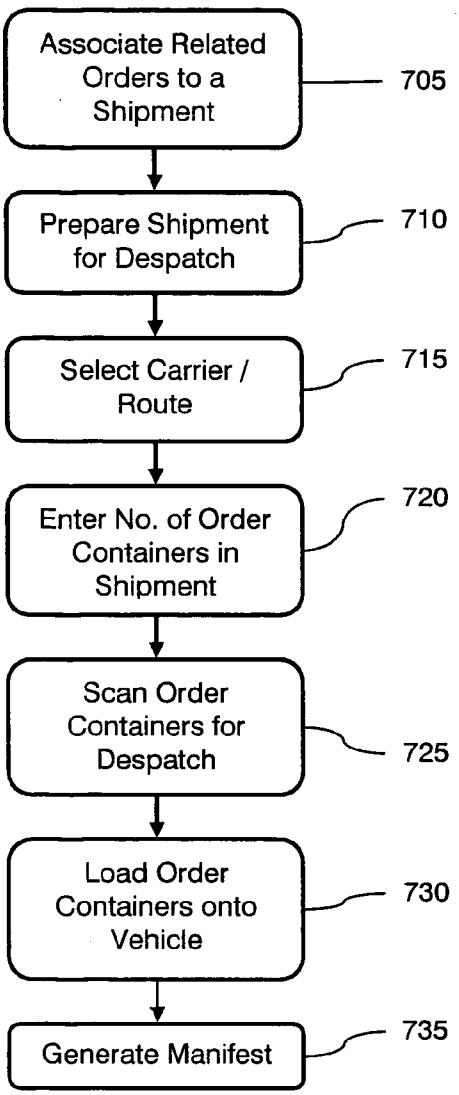

700
Associate Related Orders to a Shipment
705
Prepare Shipment for Despatch
710
Select Carrier / Route
715
Enter No. of Order Containers in Shipment
720
Scan Order Containers for Despatch
725
Load Order Containers onto Vehicle
730
Generate Manifest
735

Figure 7

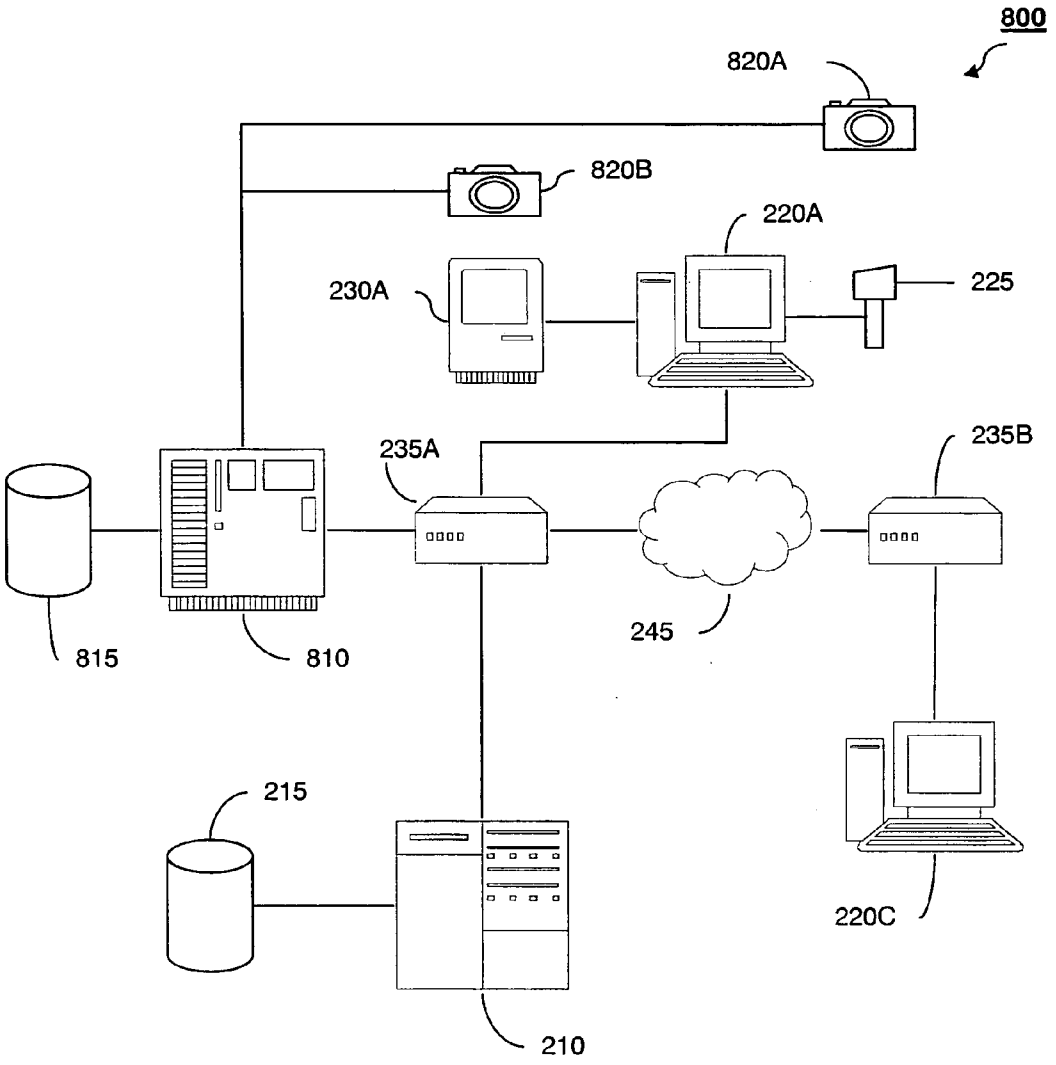


Figure 8

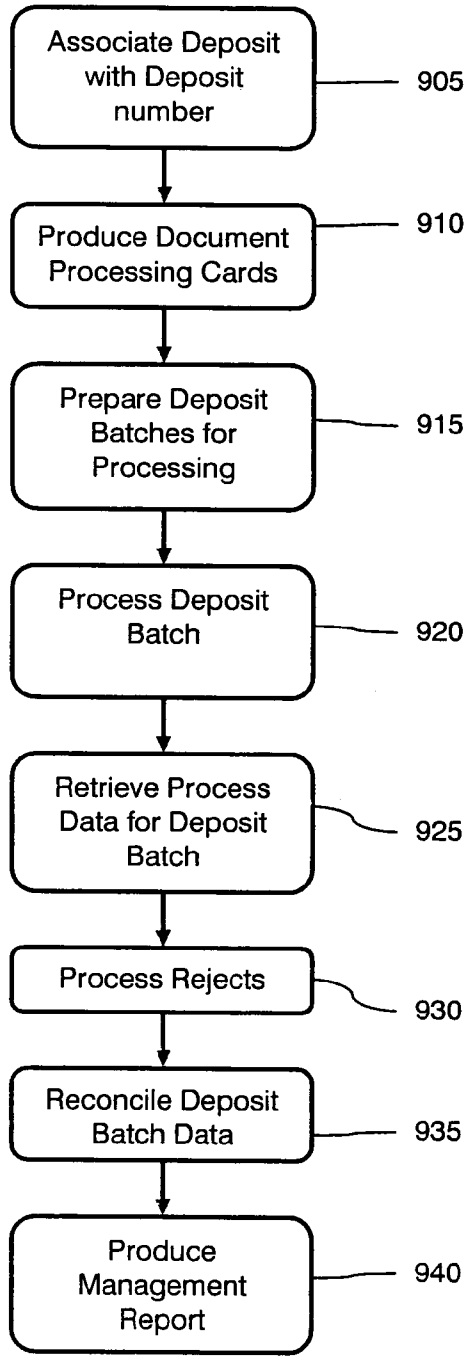

900
Associate Deposit with Deposit number
905
Produce Document Processing Cards
910
Prepare Deposit Batches for Processing
915
Process Deposit Batch
920
Retrieve Process Data for Deposit Batch
925
Process Rejects
930
Reconcile Deposit Batch Data
935
Produce Management Report
940

Figure 9

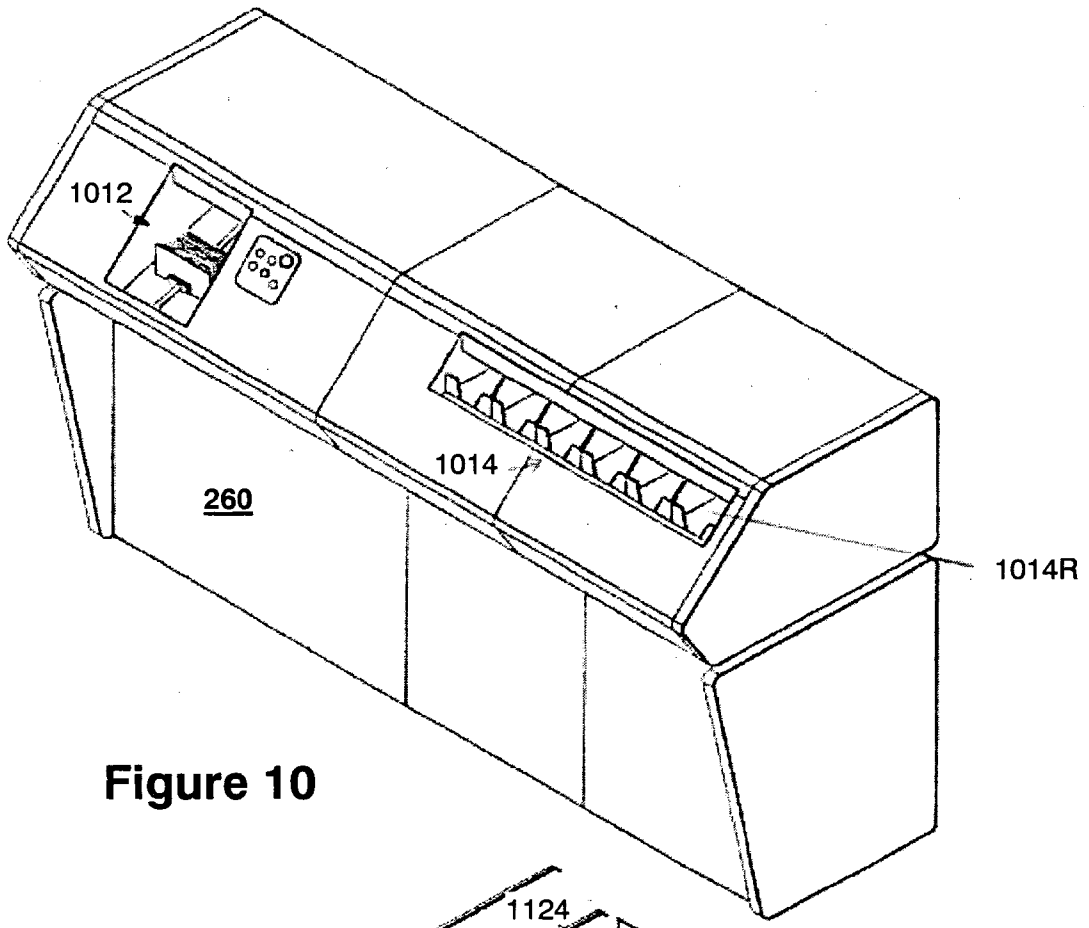


Figure 10

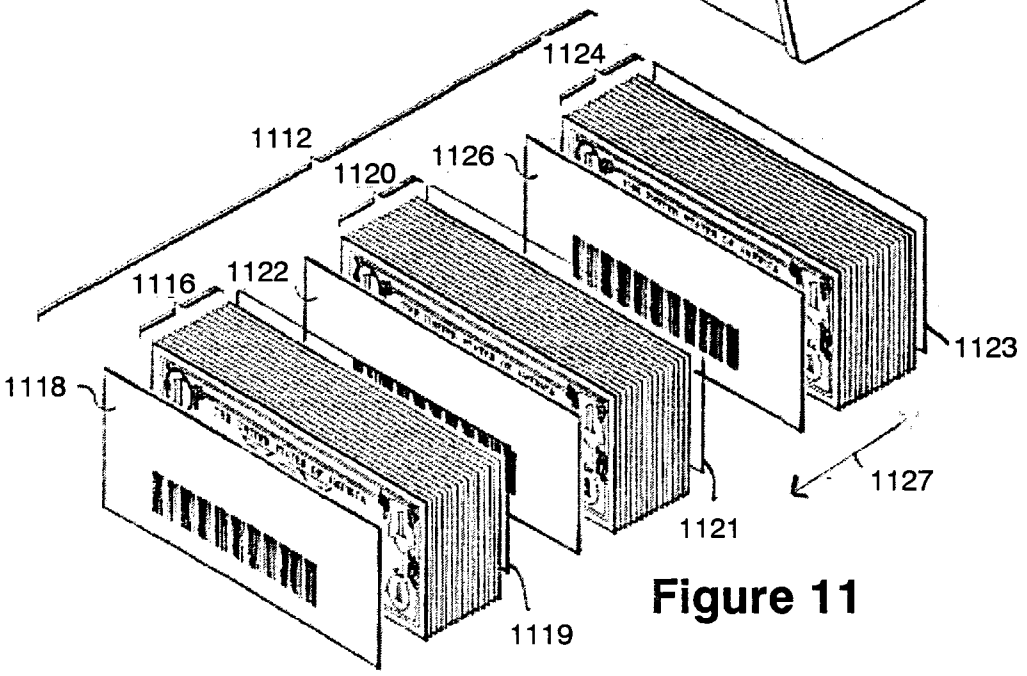


Figure 11

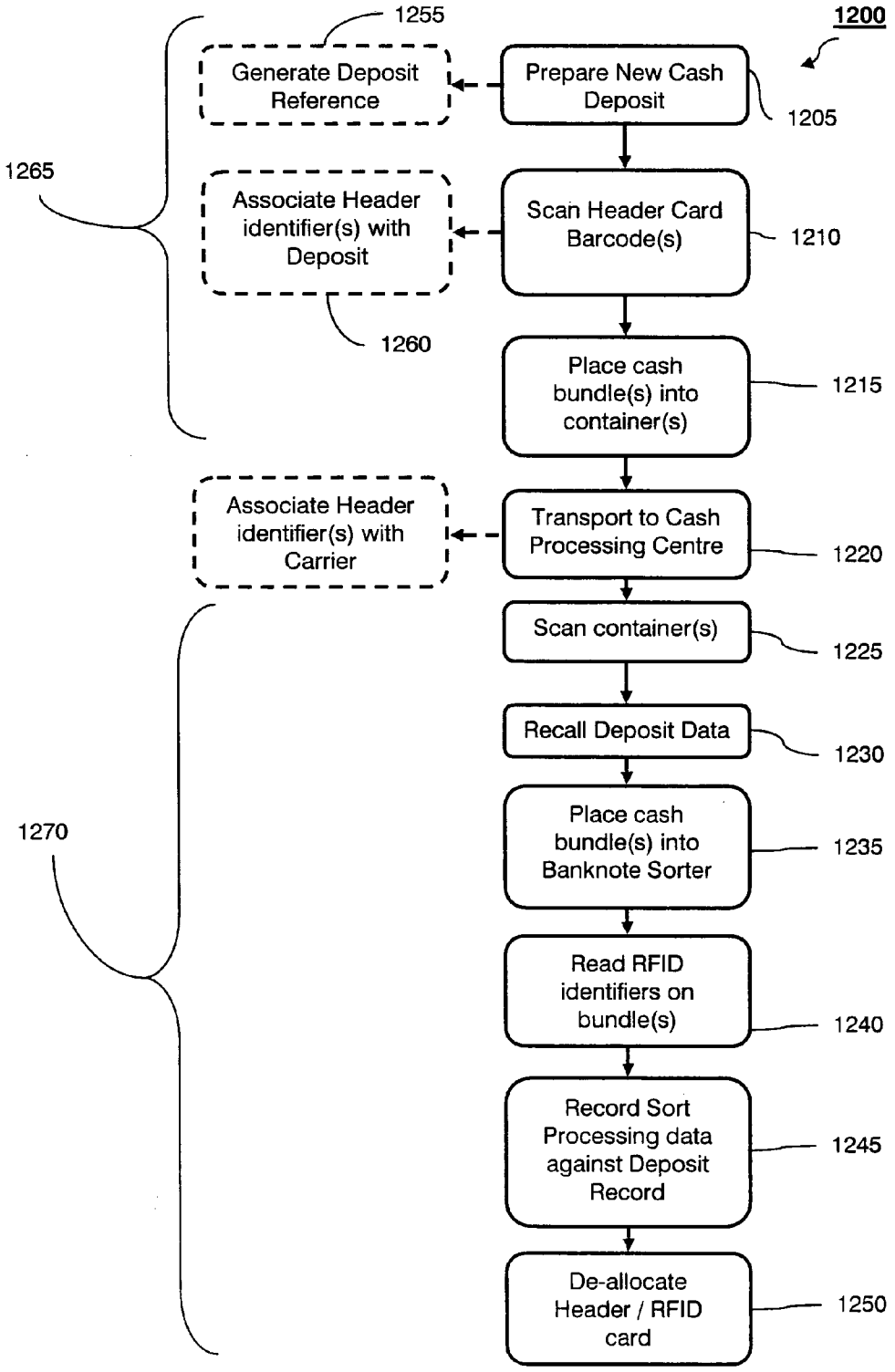

1200
Prepare New Cash Deposit
1205
Generate Deposit Reference
1255
Associate Header identifier(s) with Deposit
1260
1265
Scan Header Card Barcode(s)
1210
Place cash bundle(s) into container(s)
1215
Associate Header identifier(s) with Carrier
Transport to Cash Processing Centre
1220
Scan container(s)
1225
Recall Deposit Data
1230
1270
Place cash bundle(s) into Banknote Sorter
1235
Read RFID identifiers on bundle(s)
1240
Record Sort Processing data against Deposit Record
1245
De-allocate Header / RFID card
1250

Figure 12

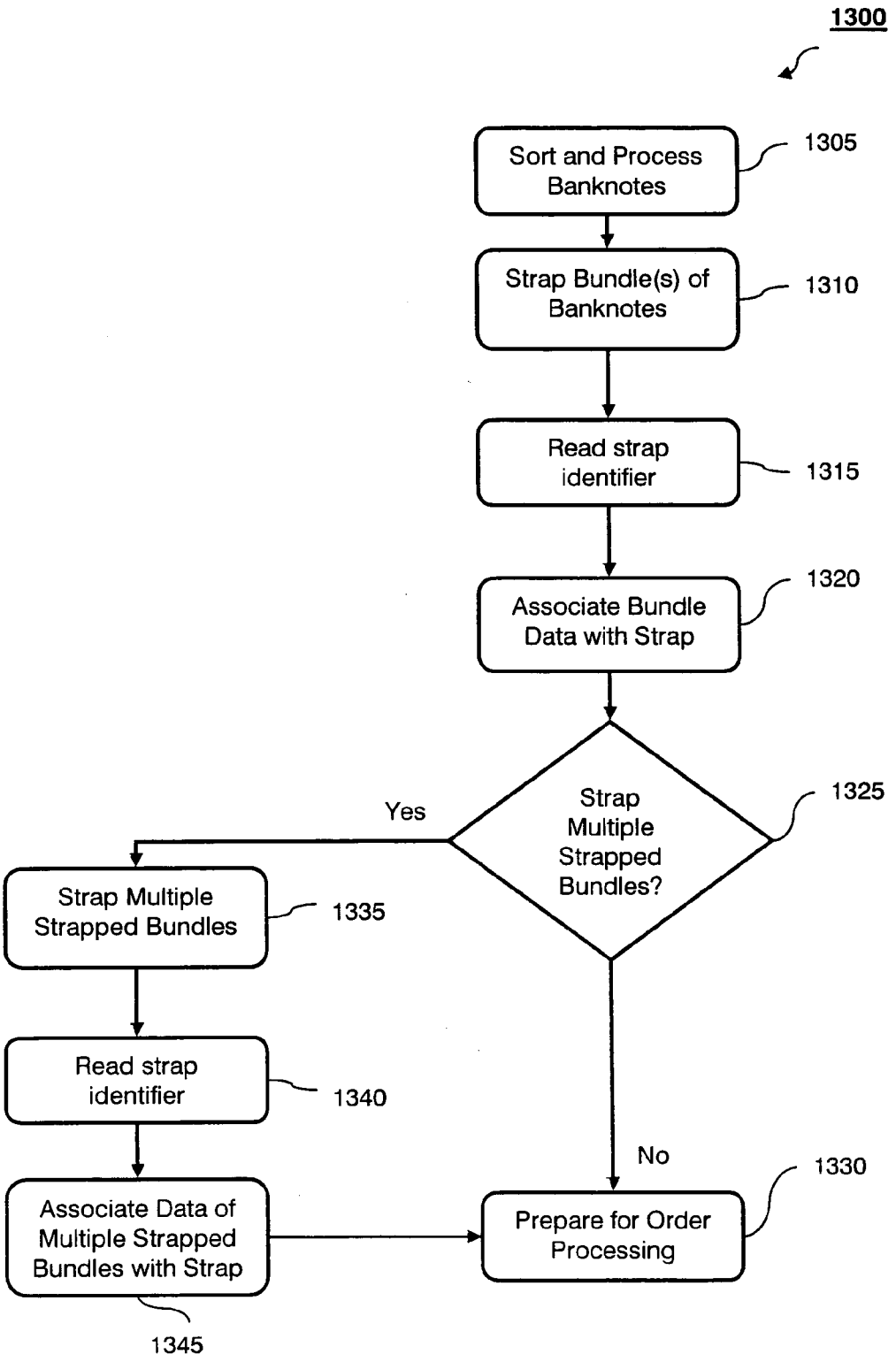

1300
Sort and Process Banknotes
1305
Strap Bundle(s) of Banknotes
1310
Read strap identifier
1315
Associate Bundle Data with Strap
1320
Strap Multiple Strapped Bundles?
1325
Yes
No
Strap Multiple Strapped Bundles
1335
Read strap identifier
1340
Associate Data of Multiple Strapped Bundles with Strap
1345
Prepare for Order Processing
1330

Figure 13

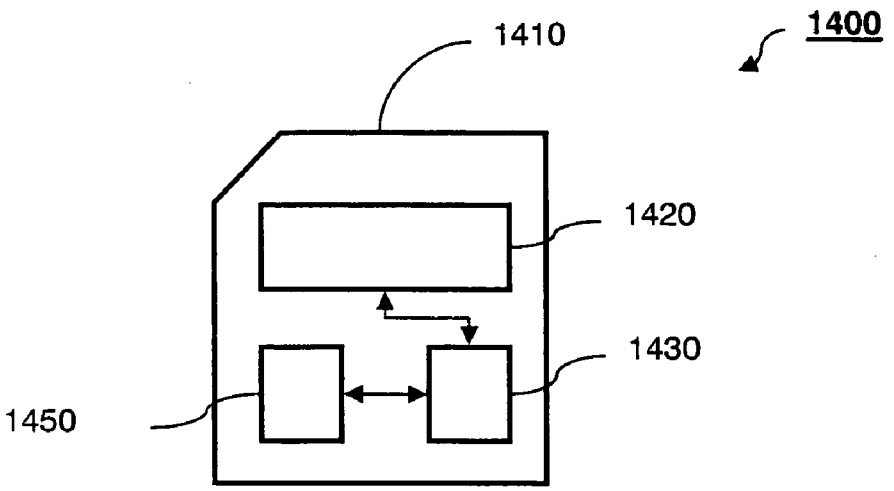


Figure 14

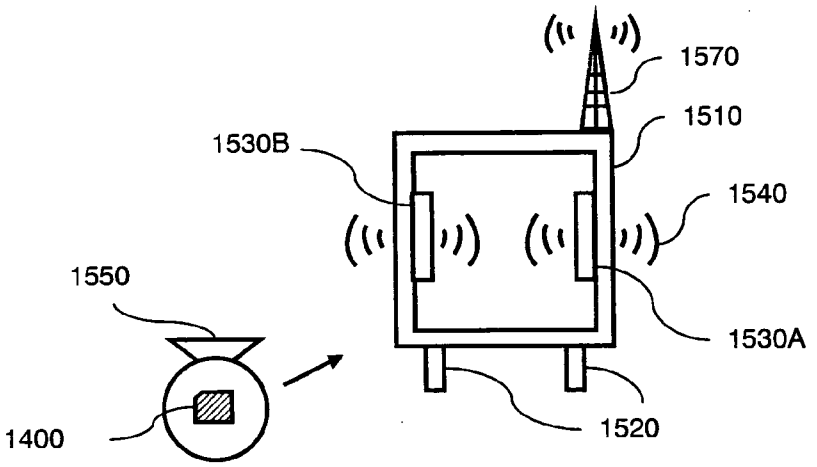


Figure 15A

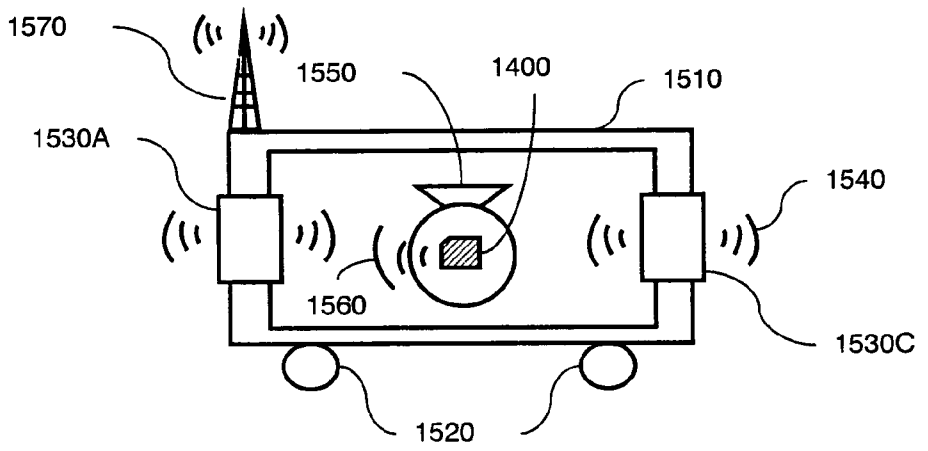


Figure 15B

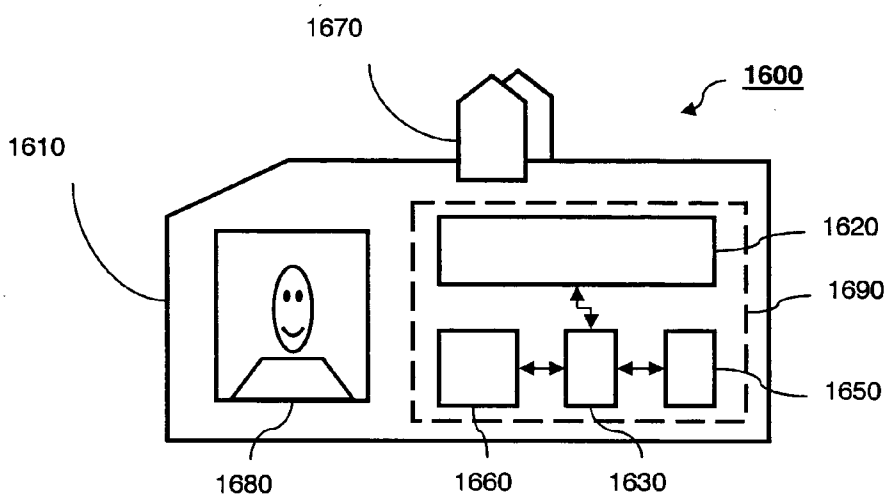


Figure 16

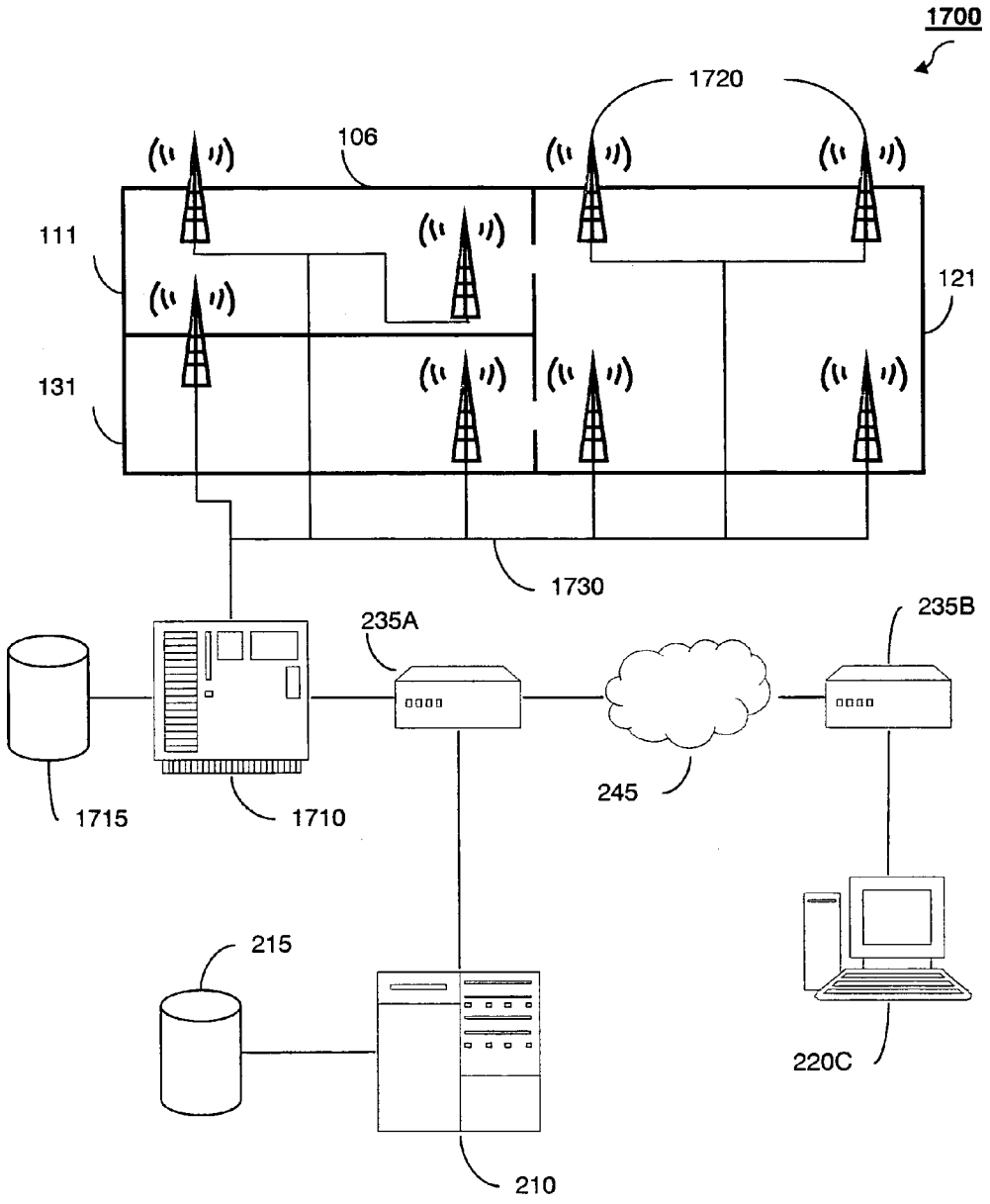

1700
1720
106
111
121
131
1730
235A
235B
1715
1710
245
215
220C
210

Figure 17

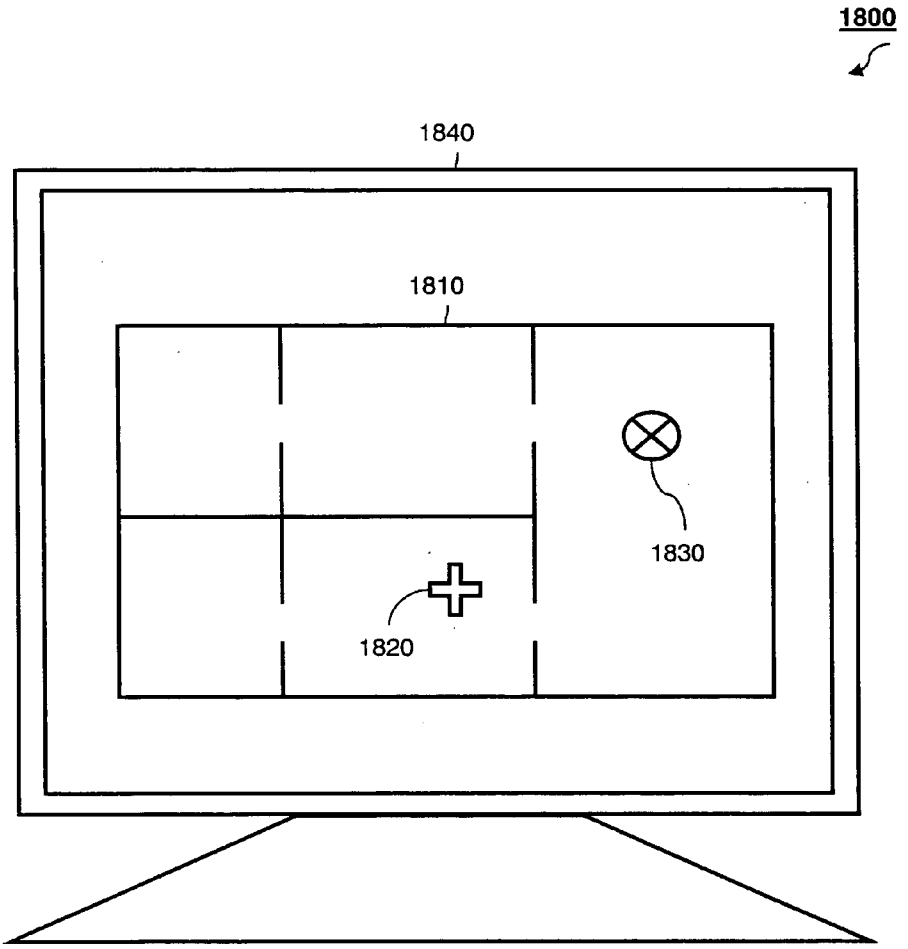


Figure 18

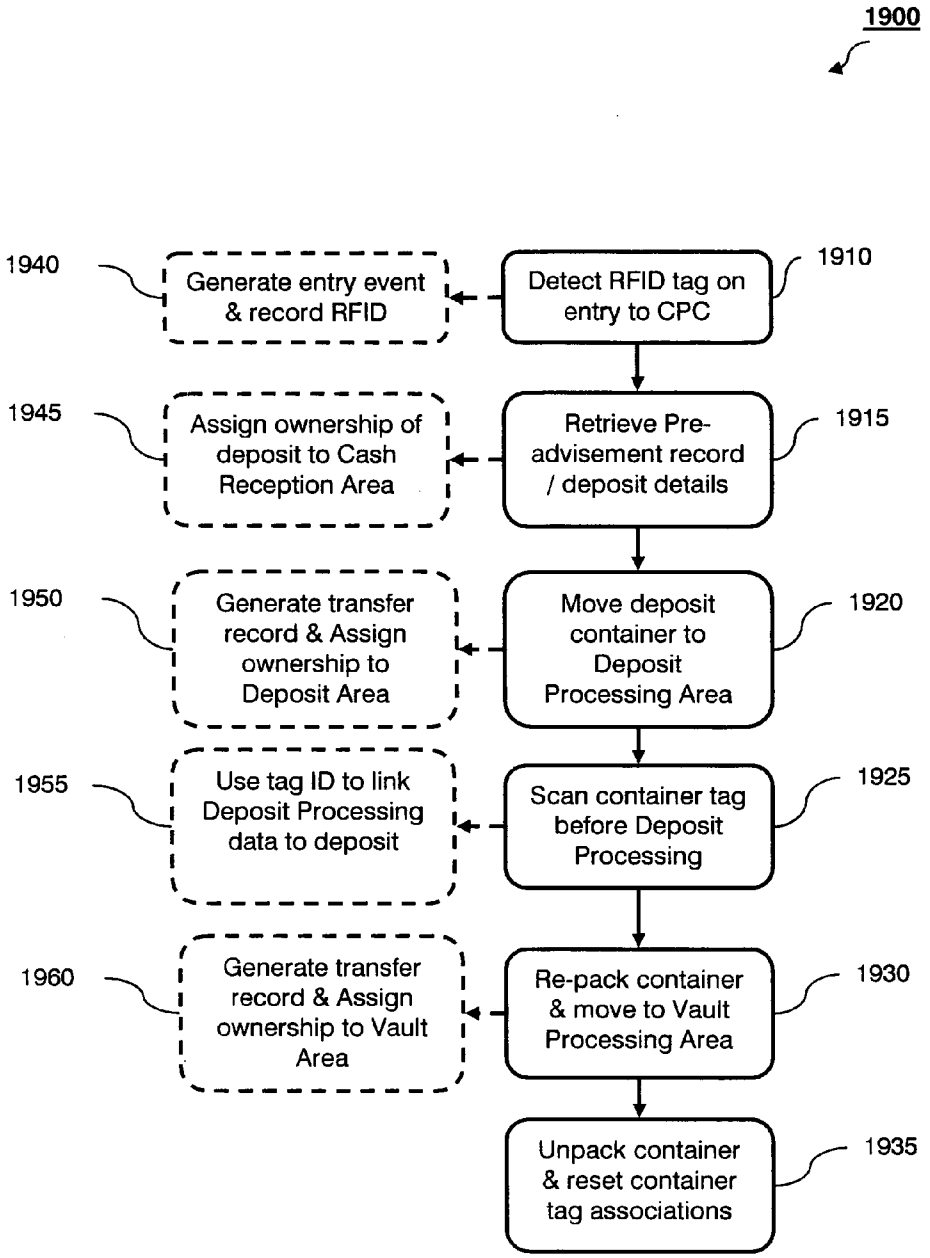

1900
1940
Generate entry event & record RFID
Detect RFID tag on entry to CPC
1910
1945
Assign ownership of deposit to Cash Reception Area
Retrieve Pre-advisement record / deposit details
1915
1950
Generate transfer record & Assign ownership to Deposit Area
Move deposit container to Deposit Processing Area
1920
1955
Use tag ID to link Deposit Processing data to deposit
Scan container tag before Deposit Processing
1925
1960
Generate transfer record & Assign ownership to Vault Area
Re-pack container & move to Vault Processing Area
1930
Unpack container & reset container tag associations
1935

Figure 19

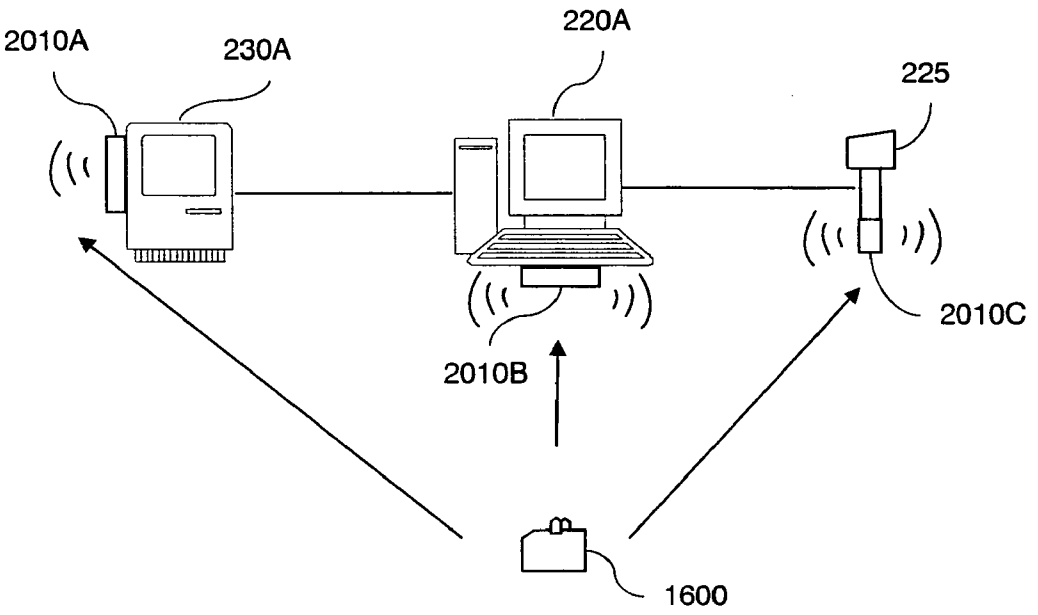


Figure 20A

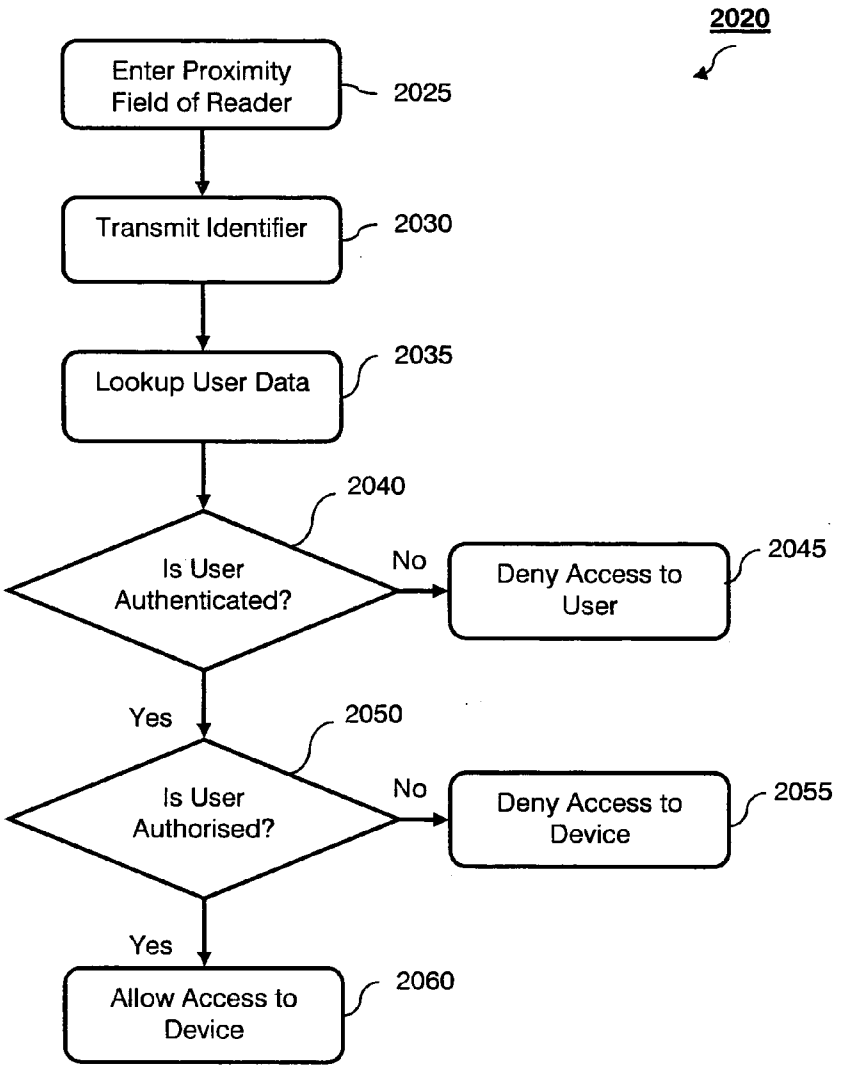

2020
Enter Proximity Field of Reader
2025
Transmit Identifier
2030
Lookup User Data
2035
2040
Is User Authenticated?
No
Deny Access to User
2045
Yes
2050
Is User Authorised?
No
Deny Access to Device
2055
Yes
Allow Access to Device
2060

Figure 20B

ENTITY MANAGEMENT METHOD AND SYSTEM USING WIRELESS DEVICES

[0001] The present invention relates to a vault management system for a cash processing centre. In particular, the present invention relates to systems and methods of efficiently managing entities within a cash processing centre using wireless devices.

[0002] The management of cash and other articles of value is vital for the functioning of a healthy modern economy. Often the processing and management of cash and other articles of value is unseen by the consumer yet plays an important role in a variety of sectors including retail, banking, gaming, and government. Most forms of management involve controlling and securing the circulation of cash, such as banknotes and coins, and other articles of value such as cheques, tokens or bonds.

[0003] The circulation of cash is typically centred on the secure deposit and storage of quantities of currency. This process is typically performed at one or more secure storage areas or vaults. These vaults may be a safe or physically secure building. Cash and other articles of value are deposited into a vault and then subsequently retrieved from the vault when required. Each vault may be owned and managed by a bank or cash management company. The vault is typically integrated into a larger cash processing centre which is further responsible for handling and verifying cash deposits and preparing cash withdrawals for delivery to customers. A cash processing centre will operate in association with cash in transit (CIT) organisations which are responsible for the security of the cash to and from the centre.

[0004] For example, a large retail establishment, at the end of a period of trading, will typically accrue a quantity of cash and other articles of value through retail transactions. As it is impractical and unsafe to keep this cash on the retail premises the cash will typically be sent to a cash processing centre, such as a bank or central deposit, using a CIT operator. The cash processing centre is then responsible for receiving the cash from the CIT operator and storing it in a safe location. Once the quantities of cash have been verified and stored, the verified total of the deposited cash may be credited to the bank account of the retail establishment. In a similar manner, at the beginning of a period of trading, a retail establishment may order a certain quantity of cash to stock the tills or points of sale. This cash will typically be provided by a suitable cash processing centre nearby. At a time stipulated by the cash order the required quantity of cash will be retrieved from the vault and sent to the retail establishment using a CIT operator. Once the cash has been retrieved from the vault and verified it may then be debited from the bank account of the retail establishment. The same processes are also used by high street banks and post offices.

[0005] When operating a cash processing centre there are several inherent problems. The first of these is the difficulty in keeping track and control of all the deposits and orders that flow through the vault. For example, a medium to large cash deposit centre may hold thousands if not millions of pounds in a vault at any one time. With such large quantities of cash it is very easy for orders and deposits to be lost or for cash to be stolen by unscrupulous employees or malicious parties. As the cash processing centre would be liable to pay out for any shortfalls in cash amount there is thus a requirement to keep track of all deposits and to prevent theft and loss.

[0006] A second problem that arises when dealing with cash processing, and which especially arises with large quantities of cash, is how to process deposits and orders in the quickest possible time. Quick processing is essential in order to prevent cash shortages in the customers requiring cash and also to prevent backlogs within the cash processing centre itself. Many cash processing centres are often constrained by the hours of opening of modern retailers and banks. For example, it is preferable for customers to send cash amounts for deposit after closing in the evening and receive cash orders before opening in the morning. Additionally, much cash processing occurs when customers are closed on the weekend. Hence there is a requirement to quickly perform a deposit and process cash orders within the cash processing centre, not only to reduce costs, but to keep the supply of cash fluid.

[0007] A third problem when dealing with cash processing in a cash processing centre is how to efficiently manage a large number of transactions whilst minimising the cash held on site. Modern large cash processing centres can receive hundreds of orders and hundreds of deposits every day requiring large amounts of available stock. If a large stock is required this will increase the attractiveness of the centre to thieves as well as require large amounts of space to be physically secured.

[0008] Unfortunately, most cash processing centres involving a vault operated using antiquated technology and procedures which are not able to address the above problems and are not able to keep up with the demands of a modern economy.

[0009] According to a first aspect of the present invention, there is provided a method of providing information about a plurality of entities within a cash processing centre, the method comprising:

[0010] coupling a first entity with a first wireless device;

[0011] coupling a second entity with a second wireless device;

[0012] reading data associated with both the first and second wireless devices;

[0013] pairing data associated with both the first and second wireless devices;

[0014] and

[0015] retrieving information concerning the relationship between the first entity and the second entity based on the pairing.

[0016] Such a method uses wireless technology to obtain information relating to two entities within a cash processing centre. The entities may be, amongst others, people, machines, computers, articles of value or containers, e.g. any objects or items that have a role within the centre. Coupling an entity with a wireless device may involve physically associating the entity with the device, for example, by attaching or electrically connecting the wireless device to the entity. The wireless devices may comprise wireless transmitters, receivers or transceivers and may use any known wireless technology, such as radio frequency communication.

[0017] Such a method enables greater control over entities within a cash processing centre and facilitates their management. The method also enables information detailing a relationship between two entities to be retrieved automatically without human intervention, for example data may be read automatically using radio frequency transceivers and may be automatically processed in conjunction with an external database to retrieve pertinent information. Such a method is important when both the first and second entities belong to

respective groups with a large number of respective entities, for example, thousands of containers and hundreds of trolleys or hundreds of employees and hundreds of client workstations. In this situation, there may be many multiple pairings and so both entities need to be identified.

[0018] The step of reading data may comprise reading data from the first wireless device and reading data from the second wireless device, wherein said data may comprise identifiers identifying the device. In certain embodiments, it may not be necessary to read an identifier from the second device, for example if its identity is known implicitly by its location within or upon the second entity. In this case the pairing may also be implicit. If the first wireless device is a transmitter and the second wireless device is a receiver, the data associated with the first device, such as a first identifier, may be read from the second device, together with data from the second device. The step of pairing data may comprise pairing the data read from the first wireless device with data read from the second wireless device, for example to produce a tuple. This tuple may be used in a database query to retrieve information concerning the relationship between the two entities, such as the distance between the two entities, whether the first entity is stored on or with the second entity or whether the first entity is authorised to use the second entity. Pairing may cover combining data from both devices in a single data item or may comprise recording data indicating that there is a link between the two entities.

[0019] In one embodiment, the first entity comprises a container for storing articles of value and the second entity comprises storage means for one or more containers. In this case, the method may further comprise: storing data comprising the properties of one or more articles of value, for example count, denomination, authentication or fitness information obtained using a banknote counter; associating said data with the first entity, for example, indexing the data using a unique identifier assigned to the first entity; storing the first entity on or within the second entity; and retrieving information comprising the cumulative properties of the articles stored on or within the second entity based on the pairing, for example, the total value of all articles of value on the storage means, or the number of counterfeit notes within the storage means. This last step may be achieved by looking up data relating to the storage means using a second identifier read from the wireless device of the storage means, such as name and location data, processing property data retrieved using a first identifier read from the wireless device of the container and displaying the aforementioned data to an operator.

[0020] In one embodiment, the first entity comprises one or more articles of value and the second entity comprises a unit adapted to store articles of value. In this case, the step of retrieving information may comprise retrieving information indicating that the first entity is stored upon the second entity.

[0021] In another embodiment, the first wireless device comprises a wireless transmitter configured to transmit a first identifier; the second wireless device comprises a wireless receiver having a second identifier; and the step of reading data comprises: transmitting the first identifier from the wireless transmitter; receiving the first identifier using the wireless receiver; and reading the first identifier received by the wireless receiver from the wireless receiver together with the second identifier, which may be stored within memory within the receiver.

[0022] In certain embodiments, the method further comprises determining signal characteristics associated with the received identifier and using the first identifier, the second identifier and the signal characteristics to determine the location of the first entity. In this case, the tuple of paired data is used by a processing system to retrieve information comprising the distance of the first entity from the second entity.

[0023] The above method may further comprise receiving the first identifier using one or more additional wireless receivers associated with respective additional entities, said wireless receivers having respective identifiers; pairing the first identifier, second identifier and the one or more additional identifiers, possibly to produce a larger tuple; and using the pairing to determine the location of the first entity, for example using triangulation techniques. Such a method may also comprise determining signal characteristics associated with each received identifier; and using the signal characteristics together with the pairing to determine the location of the first entity. This method may be regularly repeated to dynamically locate the first entity. The second entity and further entities may comprise directional receivers.

[0024] The first entity may be one of: a cage, a scanning device, an employee, one or more articles of value, a container, a trolley, or a banknote sorter.

[0025] When wireless transmitters and receivers are used the step of retrieving information may comprise determining whether the first entity is authorised to be paired with the second entity and if not generating an alert. In this case data identifying both the first and second entities may be read from wireless devices attached to said entities. This data may be paired and sent to a database to look up a relationship between the entities, for example, whether the first entity was allowed to be used with or placed upon the second entity.

[0026] In certain embodiments, the first entity may comprise an operator or a user within the cash processing centre and the step of retrieving information may comprise authenticating the operator using the first identifier, i.e. retrieving information using a tuple containing the first identifier to identify the first entity in a database.

[0027] In the method above, the second entity may comprise a device for use in the cash processing centre and the step of retrieving information further may comprise if the operator is authenticated, retrieving user data associated with the operator and based on the user data, determining whether the operator is authorised to use the device, i.e. using the second identifier to identify the second entity in the database and then, once identified, looking for predetermined configurable relationship information concerning the particular two entities. This method may further comprise, if the operator is authorised, allowing access to the device, or if not, denying access to the device and optionally generating an alert. The step of determining whether the operator is authorised to use the device may comprise determining whether the operator is authorised to use any further devices connected to the device; and if so, allowing access to the authorised further devices.

[0028] The device may comprise one of: a banknote counter or sorter, a client computing device, or a handheld electronic device.

[0029] The wireless devices may comprise radio frequency identification devices.

[0030] The first entity may belong to a first group of entities and the second entity may belong to a second group of entities.

[0031] According to a second aspect of the present invention there is provided a system for providing information about plurality of entities within a cash processing centre comprising:

[0032] a first wireless device coupled to a first entity;

[0033] a second wireless device coupled to a second entity; and

[0034] a processor adapted to:

[0035] read data associated with both the first and second wireless devices;

[0036] pair data associated with both the first and second wireless devices; and

[0037] retrieve information concerning the relationship between the first entity and the second entity based on the pairing.

[0038] The first entity may comprise a container for storing articles of value; and the second entity may comprise storage means for one or more containers. In this case, the processor may be further adapted to retrieve information comprising the cumulative properties of the articles stored on or within the second entity based on the pairing, optionally from a database coupled to the processor.

[0039] Alternatively, the first entity may comprise one or more articles of value and the second entity may comprise a unit adapted to store articles of value. In this case, the processor may be further adapted to retrieve information indicating that the first entity is stored upon the second entity.

[0040] In one embodiment, the first wireless device comprises a wireless transmitter configured to transmit a first identifier and the second wireless device comprises a wireless receiver having a second identifier. In this case the processor may be further adapted to read a first identifier received from the second wireless device, together with the second identifier of said device, and pair said identifiers.

[0041] In a first variation, the processor is further adapted to receive signal characteristics associated with the received first identifier; and process the first identifier, the second identifier and the signal characteristics to determine the location of the first entity. In this case, the system may further comprise one or more additional wireless receivers associated with respective additional entities, said wireless receivers having respective additional identifiers. The processor may then be further adapted to receive one or more copies of the first identifier as received by one or more of the additional wireless receivers, together with the additional identifiers of said receivers, pair the first identifier, second identifier and the one or more additional identifiers; and determine the location of the first entity using the pairing. In certain implementations, the processor is adapted to also receive signal characteristics from each wireless receiver; and process the signal characteristics together with the pairing to determine the location of the first entity, possibly repeating the processing steps at regular intervals to dynamically update the location of the first entity. The wireless receivers may comprise directional receivers and the processor may be adapted to determine the location of the first entity using triangulation. In this case, as well as reading identifiers from the devices, extra information such as the signal strength of the received first identifier, as received by a wireless receiver identified by a second identifier is read. In this case, the processor may retrieve further information from a location processing module or from another process being implemented by the processor.

[0042] The first entity may be one of: a cage, a scanning device, an employee, one or more articles of value, a container, a trolley, or a banknote sorter.

[0043] The system may further comprise a database, for example a database comprising authorisation data. The processor may then be adapted to access the database to determine whether the first entity is authorised to be paired with the second entity; and if not generate an alert. In this case, the information concerning the relationship comprises the authorisation data.

[0044] In a particular embodiment, the first entity comprises an operator within the cash processing centre and/or the second entity comprises a device for use in the cash processing centre. The system may then further comprise authorisation/authentication stored in a database. The processor may then be further adapted to access the database to authenticate the operator using the first identifier and/or retrieve authorisation data associated with the operator from the database if the operator is authenticated. Based on the authorisation data, it can be determined whether the operator is authorised to use the device. The processor may be further adapted to: allow access to the device if the operator is authorised, or deny access to the device if the operator is not authorised; and optionally generate an alert if the operator is not authenticated and/or authorised.

[0045] The device may comprise one of: a banknote counter or sorter, a client computing device, or a handheld electronic device.

[0046] The system may also further comprise one or more further devices connectable to the second entity and the processor may be further adapted to, based on the authorisation data, determine whether the operator is authorised to use any of said further devices and allow access to any connected further devices if the operator is authorised.

[0047] According to certain embodiments a method of tracking one or more articles within a cash processing centre, the cash processing centre comprising a plurality of receivers for radio frequency communication may be provided. This method comprises:

[0048] a. coupling a radio frequency identification device to an article, the radio frequency identification device having an unique identifier;

[0049] b. receiving a radio frequency signal from the radio frequency identification device at at least two receivers, the radio frequency signal comprising the unique identifier;

[0050] c. using the received radio frequency signal, together with the received unique identifier, to determine the location of the radio frequency identification device; and

[0051] d. updating the location of the article based on the location of the radio frequency identification device.

[0052] In some embodiments the method above uses trilateration, wherein the cash processing centre comprises at least three receivers for radio frequency communication and the method further comprises: receiving a radio frequency signal from the radio frequency identification device at at least three access points; and using the signal strength of the received radio frequency signal received at each receiver, together with the received unique identifier, to determine the location of the radio frequency identification device. In other embodiments the receivers comprise directional receivers and step c) comprises determining the location of the radio frequency device using triangulation. The located article may be one of: a cage,

a scanning device, an employee, one or more articles of value, a container, a trolley, or a banknote sorter.

[0053] According to certain embodiments there is provided a storage unit for containers for use in a cash processing centre, the containers containing one or more articles of value, the storage unit comprising:

[0054] a storage area for one or more containers,

[0055] the storage unit characterized by:

[0056] one or more radio frequency reading devices configured to wirelessly read data from a radio frequency identification device;

[0057] wherein, in use, each container has an associated radio frequency identification device, the radio frequency identification device storing data associated with properties of the articles of value within the container; and

[0058] in use, the properties of any articles of value stored upon the storage unit may be retrieved by processing data read by the one or more radio frequency reading devices.

[0059] According to certain embodiments there is provided a method of tracking articles of value within a cash processing centre comprising:

[0060] a. coupling one or more articles of value with a first radio frequency identification device;

[0061] b. coupling a unit adapted to store articles of value with a second radio frequency identification device;

[0062] c. reading data associated with both the first and second radio frequency devices; and

[0063] d. recording that the one or more articles of value are stored upon the unit based on the read data.

[0064] Several examples of a number of methods and systems according to the present invention will now be described with reference to the accompanying drawings, in which:

[0065] FIG. **1**A is a process diagram of an exemplary cash processing cycle according to a first embodiment of the present invention;

[0066] FIG. **1**B is a process diagram of an exemplary extended cash processing cycle according to a second embodiment of the present invention;

[0067] FIG. **1**C is a schematic diagram of an exemplary cash processing centre configured to implement the first embodiment of the present invention;

[0068] FIG. **1**D is a schematic diagram of an extended exemplary cash processing centre configured to implement the second embodiment of the present invention;

[0069] FIG. **1**E is a schematic diagram of an alternative extended exemplary cash processing centre configured to implement the second embodiment of the present invention;

[0070] FIG. **2**A is a diagram illustrating an exemplary hardware configuration for implementing the first embodiment of the present invention;

[0071] FIG. **2**B is a diagram illustrating an exemplary hardware configuration to implement the fourth embodiment of the present invention;

[0072] FIG. **3**A is a flow chart demonstrating an exemplary transfer process according to the first and second embodiments of the present invention;

[0073] FIG. **3**B is a flow chart demonstrating an exemplary acknowledgement process according to the first and second embodiments of the present invention;

[0074] FIG. **4** is a flow chart demonstrating an exemplary cash reception process according to the second embodiment of the present invention;

[0075] FIG. **5**A is a flow chart demonstrating an exemplary cash deposit operation according to a first embodiment of the present invention;

[0076] FIG. **5**B is a flow chart demonstrating an exemplary count operation according to a first embodiment of the present invention;

[0077] FIG. **6** is a flow chart demonstrating an exemplary cash order processing operation according to a first embodiment of the present invention;

[0078] FIG. **7** is a flow chart demonstrating an exemplary cash despatch operation according to the second embodiment of the present invention;

[0079] FIG. **8** is a diagram illustrating an exemplary hardware configuration of a third embodiment of the present invention;

[0080] FIG. **9** is a flow chart demonstrating an exemplary deposit processing operation according to a fourth embodiment of the present invention;

[0081] FIG. **10** is a diagram illustrating an exemplary currency sorting machine for implementing the exemplary deposit processing operation of FIG. **9**;

[0082] FIG. **11** is a diagram illustrating a typical stack of banknotes used in the exemplary deposit processing operation of FIG. **9**;

[0083] FIG. **12** is a flow chart demonstrating an exemplary deposit processing operation according to a fifth embodiment of the present invention;

[0084] FIG. **13** is a flow chart demonstrating an exemplary processing operation according to a sixth embodiment of the present invention;

[0085] FIG. **14** is a diagram illustrating an exemplary radio frequency identification chip;

[0086] FIGS. **15**A and **15**B are diagrams respectively illustrating a front and side view of an exemplary storage unit for use within a cash processing centre;

[0087] FIG. **16** is a diagram of an exemplary employee badge incorporating a radio frequency identification device;

[0088] FIG. **17** is a diagram illustrating an exemplary hardware configuration of a wireless trilateration system;

[0089] FIG. **18** is a diagram illustrating an exemplary workstation running a location module;

[0090] FIG. **19** is a flow chart illustrating an exemplary tracking method using a radio frequency identification device;

[0091] FIG. **20**A is a diagram illustrating an exemplary system for authenticating and authorising an employee using a radio frequency identification device; and

[0092] FIG. **20**B is a flow chart illustrating an exemplary authentication and authorisation method using the system of FIG. **20**A.

[0093] FIG. **1**A displays a number of processes involved in the management of a vault within a cash processing centre according to a first embodiment of the present invention. The cash processing cycle **100** therein is configured to complement the typical physical layout of a cash processing centre. The cash processing centre may be run by a variety of organisations. These include central banks, commercial banks, cash in transit (CIT) companies and transport and leisure companies. A schematic diagram of the ground plan of an exemplary cash processing centre is shown in FIG. **1**C. This ground plan is provided as an example only and other differing cash processing centre designs may also be used with the management processes of the present invention. Cash deposit centre **105** comprises secure vault area **121**, deposit area **111** and order

processing area **131**. The secure vault area **121** may comprise, but is not limited to, a safe, a physically secure room or a physically secure area. The deposit area **111** is an area for preparing cash for deposit into the vault and the order processing area **131** is an area for preparing cash orders. The deposit area **111** and the order processing area **131** are separated from the vault area **121** by a physical boundary **141**. Physical boundary **141** has two respective openings: entry point **116** into the vault area **121** and exit point **126** into the order processing area **131**. These entry and exit points may be provided by one way doors or other suitable secure gateway apparatus. Deposit area **111** may also be separated from order processing area **131** by physical boundary **142**, although in some implementations the two areas may comprise a single room.

[0094] The cash processing cycle **100** has three processes that are typically performed in the three respective areas of FIG. **1**C. However, it is possible that all three processes may be carried out within the secured boundary of the vault. The cash processing cycle **100** first comprises deposit processing **110**. This step is typically performed in the deposit area **111**, wherein cash and other articles of value are prepared for deposit into the vault or secure area **121**. This preparation may involve: unloading cash from containers; counting, verification and validation; and preparing the cash in a suitable form for deposit, such as bundling the notes in set quantities of denominations. The articles for deposit may comprise articles of value such as coins, banknotes, cheques, tokens or bonds. The flow of cash into vault is illustrated by arrow **115**. This represents the physical passage **117** of cash from the deposit area **111** to the vault **121** via entry point **116**. Boundary line **140** represents a figurative boundary between the stage of deposit processing **110** and the vault processing **120**. Boundary line **140** may reflect the physical boundary **141** between the deposit area **111** and the vault **120** or may simply be a means of delimiting the two processes. The figurative boundary is used as part of the transfer process described in relation to FIG. **3**.

[0095] The cash processing cycle **100** next comprises vault processing **120**. At this stage cash received by the vault **121**, for example via entry point **116**, may be further counted, verified and validated and placed in bundles of denominations suitable for storage. The vault **121** may comprise one or more cash deposit apparatus such as a TCR (Teller Cash Recycler) Twinsafe or "Vertera" (TM) apparatus supplied by De La Rue International. Alternatively, the vault **121** may comprise a regular safe or vault, wherein documents of value are routed in and out of the safe or vault by hand. In this case vault processing **120** may involve depositing received cash into a suitable deposit apparatus. Cash remains in the vault **121** until it is required to fulfil a cash order. At this point the vault processing **120** involves preparing the required amount of cash to send for order processing **130**. The flow of cash from the stage of vault processing **120** to the stage of order processing **130** is represented by arrow **125** and again involves the crossing of figurative boundary **140**. This transfer **125** may reflect the physical removal **127** of cash from a safe or secure area **121** via exit point **126** and the transfer of this cash across physical boundary **141** to the order processing area **131**.

[0096] The third stage of the cash processing cycle **100** is order processing **130**. At this stage, quantities of cash are prepared to supply customers, such as, amongst others, retailers and banks. A cash order may be scheduled regularly in the manner of a standing order or may be prepared individually based on a received order. The quantity of cash received from the vault area **121** will typically be counted, bundled and placed in suitable containers or bags for delivery.

[0097] An example of suitable hardware that may be used to implement the present invention is illustrated in FIG. **2**A. Vault management system **200** comprises a vault management server **210** upon which the vault management software operates. The vault management server **210** is operably connected to database **215**. The database may be stored on one or more local or remote storage mediums or devices. Typically, vault management server **210** comprises a standard hardware configuration running Microsoft Windows 2000/2003 or an Oracle-supported host and database **215** comprises an Oracle or SQL Server compatible database. However, any suitable software platform known in the art may be used to implement the invention. The processes used to generate data records and populate the vault management database are discussed subsequently. Sources of data include, but are not limited to, order forecasting systems, high-speed banknote sorters, coin sorters, desktop banknote and coin sorters, document capture systems, CIT providers, remote bank and/or store locations. The vault management database may also be adapted to interface with internal or external accounting or data warehousing systems.

[0098] Vault management server **210** typically further comprises a network adapter to connect to a wired or wireless network **231**, using standards such as Ethernet or 802.11g. Network **231** is typically a local area network (LAN) covering the cash processing centre **105**. In FIG. **2**A network **231** comprises a first network hub **235**A connected to a second network hub **235**B over a wide area network (WAN) **245**. Vault management server **210** may be connected to first network hub **235**A via a LAN connection as shown in FIG. **2**A or alternatively may be located remotely to the cash processing centre **105** and connected to first network hub **235**A via a WAN connection. The network **231** is presented as an example and any suitable form of network topology may be used in practice. Network hub **235**A is connected to a number of networked devices **220** and **230** and these network connections may also be wired or wireless using known protocols. The network may also be secured using methods known in the art.

[0099] Networked devices **220** and **230** comprise networked client workstations **220**A and **220**B. Such workstations are typically located in the areas of the cash processing centre **105** shown in FIG. **1**C: for example workstation **220**A may be located in deposit area **111** and client workstation **220**B may be located in order area **131**. Additional peripherals may also be connected to client workstations **220**. In FIG. **2**A client workstation **220**A is connected to barcode reader **225** and client workstation **220**B is connected to print device **240**. Any number of peripherals may be connected to a client workstation using any known protocols.

[0100] A number of banknote counters **230** may also be connected to the network **231**, either through client workstations **220**A and **220**B or through using a banknote counter **230**B with network capability, such as counter **230**B, connected to the network **231** via network hub **235**. These banknote counters may be a 2600, EV86, Evolution™, nVision or Kalebra model counter manufactured by De La Rue International Limited or may be any suitable one, two or three or more pocket counter that is adapted to count, validate and/or

process batches of banknotes. Networked banknote counter **230**B may be located in the any of the cash processing centre areas shown in FIG. **1**C.

[0101] The example shown in FIG. **2**A is for illustrative purposes only and the number of client workstations **220** and/or counting devices **230** may vary according to the particular cash deposit centre involved. For example, the deposit area **111** may comprise two or more client workstations **220**A wherein each workstation is connected to a barcode reading device **225** and a print device such as print device **240**. Alternatively the deposit area **111** may comprise a plurality of banknote counters **230** all connected to network **231**.

[0102] Vault management system **200** may also comprise a remote client workstation **220**C as shown in FIG. **2**A. This is an optional feature and need not be included in all implementations. This workstation is connected to hub **235**B which is connected to the network **231** via a wide area network **245** such as the Internet. Typically, security will be enforced by using a virtual private network (VPN) operating on top of standard communication protocols, such as TCP/IP. Client workstation **220**C then allows access to the vault management software running on server **210** from a remote location.

[0103] Client devices **220** may be any suitable client device known in the art. For example each device could comprise: a personal computer, a thin client workstation, a personal digital assistant (PDA), a smart phone, a cellular phone, a laptop, a multimedia device etc. Typically, such a device comprises data processing and data transfer means. In this description any functionality and/or interfaces provided by client devices **220** are assumed to be appropriately formatted for the hardware of the device. For example, a graphical user interface (GUI) may be implemented in Java with data supplied in eXtended Markup Language (XML) format; in which case there are known techniques to provide said interface and data on a variety of devices from a personal computer to a cellular or mobile telephone.

[0104] The vault management system of the present invention is implemented using a number of integrated software modules that correspond to each of the processing stages illustrated in FIG. **1**A. For example, a system based on FIG. **1**A comprises three modules corresponding to stages **110**, **120** and **130**. These software modules may be wholly or partly implemented as software processes or interfaces running on vault management server **210**. Each client workstation **220** is able to connect to the vault management server **210** and maybe a fat or thin client. Each module typically has its own user interface, typically a graphical user interface (GUI), that is presented to an operator working upon one of the client workstations **220**. Each workstation **220** may be restricted to only show the GUI relevant to the area in which the workstation is located, for example workstation **220**A may be restricted to only show an operator the GUI associated with the deposit processing module. Each module allows the system to acquire data related to one of the three processing stages, the data being acquired by processes performed by an operator interfacing with the GUI of the relevant module.

[0105] As well as a suite of modules corresponding to each of the cash management processes of FIG. **1**A the vault management software may also optionally comprise a number of additional modules that enable customisable configuration and provide standing data used by the system. These modules may be one or more of: a security module for managing user access and authorisation levels; a definitions module to manage administration of specific terminology and fixed data; a GUI configuration module to manage the appearance, behaviour and dynamics of each GUI; and a customer database to manage customer specific data reference by the vault management software.

[0106] The GUIs used by the present invention may be pre-designed or may be generated at run-time (i.e. when the vault management system is implemented) from standard controls and components. During development, maintenance or enhancement of the system, one or more user interface "wizards" or guided processes may be provided. These enable non-technical personnel to design interfaces and reduce production times for qualified developers. Each GUI may be further configurable during implementation by selecting controls and components from menus and lists. Certain configuration options may be disabled for certain users.

[0107] In certain embodiments of the present invention, the vault management server **210** may be a virtual server, i.e. may be implemented above an underlying host system. This enables the processes of the vault management server **210** to be distributed over one or more physical computers and the processes of the server to be accessed from one or more remote terminals. The physical computers implementing the virtual server may also host one or more additional systems, for example CCTV server **810** as described with reference to FIG. **8**. Such a system facilitates access from portable devices and remote thin clients and enables the vault management server **210** to be implemented in an enclosed environment that can be easily shut down and modified without affecting underlying systems. Such virtual platforms may be provided by Citrix Systems Incorporated of Florida, USA or Microsoft Corporation of Washington, USA.

[0108] The operations performed in the deposit processing **110** will now be described in relation to FIGS. **5**A and **5**B. The deposit processing **110** is performed on one or more quantities of cash that have been received from outside of the cash processing centre. The cash is received in one or more containers that can vary in size and form. These containers may be organised in a nested hierarchy. For example, the cash processing centre may use cages, bulk bags and satchels, wherein a cage may hold one or more bulk bags and a bulk bag may contain one or more satchels. Alternatively, the cash processing centre may use containers, bags and envelopes or a combination of all six container types. Each of the containers may have its own individual identifier, for example in the form of a serial number encoded within a barcode present on the outside of the container.

[0109] Each received quantity of cash has an associated deposit slip. This deposit slip lists one or more properties related to the received cash, for example, the originating customer or depositor, the declared deposit amount and the date of deposit. Each container containing a quantity of cash also contains a deposit slip. Containers containing other containers may also contain deposit slips relating to the cumulative deposit amount of all contained containers. The deposit slip may also further comprise a one or two dimensional barcode. This barcode may encode a serial number or actual deposit information. At the deposit stage the quantity of cash within each container is linked to the depositor and verified against the deposit amount declared on the deposit slip.

[0110] FIG. **5**A shows a method for obtaining the deposit data associated with a deposit. At step **505** an operator logs into the deposit module using a client workstation, such as workstation **220**A. The login procedure may involve entering a user name and password. In some embodiments the work-

station **220**A may be connected to a biometric device adapted to read a biometric identifier associated with the operator. This identifier may be a finger print, a finger or palm vein structure, an iris scan or a voice print (amongst others). Hitachi Ltd provides a number of reading devices which may be used to read the biometric identifier. The biometric identifier is then used instead of a username and/or password to log in to the relevant software module.

[0111] The operator then selects a deposit container for deposit processing **510**, opens the container and retrieves the deposit slip. A new deposit record is then created if no pre-existing record exists. The information present on the deposit slip is then obtained **515** using one or more of automatic means, for example scanning a barcode **515**A present on a deposit slip or applying optical character recognition (OCR) to a captured image of the deposit software, or using manual means, for example entering the information **515**B, **515**C into the deposit module GUI. As a deposit operator will regularly spend a large proportion of their time entering deposit information all functions within the deposit module are accessible with keystrokes or by assigning hot keys. If a barcode is present then the operator can use a barcode scanner **225** to either retrieve a serial number or the deposit data itself. A serial number may be linked to a deposit record generated by the depositing customer or may identify the depositor. Other data that maybe recorded include a till, cashier, store or branch identifier. Once the depositor information has been entered then the deposit record is updated **520**. If it is not assigned already the cash deposit is assigned to the current operator by associating an operator identifier, such as a user name, with the deposit record. This may be achieved by associating the user name of the current active operator with the deposit record. A cash deposit may also be assigned to an area, for example deposit area **111**, as well as, or instead of an operator. This makes the current operator and/or area responsible for the cash deposit until a transfer is performed.

[0112] The data present on the deposit slip may also be obtained using pre-advisement. Pre-advisement involves the customer pre-advising the cash processing centre on the nature of a deposit. Typically, this may be performed using a web interface wherein the customer enters the deposit amount and container identifiers while preparing the deposit. In other embodiments, this may be performed using Interactive Voice Response (IVR) technology. This deposit data is then linked to the cash processing centre receiving the deposit. When a container is subsequent sent and received by the cash processing centre the pre-entered deposit information can be retrieved upon container identification, e.g. when the containers making up the deposit are scanned by an operator.

[0113] After initial deposit processing a count and verification process begins. The count and verification process is illustrated in FIG. **5**B and is performed by an operator interacting with an adapted GUI of the deposit module. The method **501** begins at step **520** with the retrieval of cash, typically in the form of banknotes, from the selected deposit container. The cash is then counted at stage **535**. Counting may be performed manually or, as is typically the case, may be performed by an on-line or off-line banknote counter **230**. If the cash processing centre is configured to receive and process cheques then cheque imaging systems and software may also be integrated into the vault management system to provide count information for cheque deposits.

[0114] In a manual count the operator counts and inspects the cash from the container and enters the results of the count into the deposit module GUI. Typically, the cash is sorted into a number of denominations and the total number of notes and cash value of each denomination is recorded. The fitness of each note can also be inspected and the serial numbers recorded. If a banknote counter **230**A is currently connected to the client workstation **220** at which the current operator is operating, i.e. is on-line, this will be shown within the deposit module GUI and the banknote counter can be used to generate data documenting characteristics of counted notes. These can be, amongst others, denomination, fitness, and authentication characteristics. To use an on-line banknote counter the operator places the retrieved banknotes on banknote counter **230**A. The banknote counter **230**A is then able to count and/or verify the banknotes and the data generated by the banknote counter **230**A is sent back to the client workstation **220**A to populate the count data at stage **540**. Alternatively banknote counter **230**A can be disconnected from the client workstation **220**A, i.e. used off-line. In this case the banknotes will still be counted by the banknote counter but the operator will manually enter the data on the banknote counter display. If the banknote counter **230**A is adapted to authenticate the banknotes and identify counterfeit notes then data related to counterfeit notes may either be passed automatically to the deposit module from the banknote counter if the counter is on-line or may otherwise be manually entered into the adapted deposit GUI based on data presented to the user on the banknote counter display. Data on counterfeit notes can then be printed by a user or supervisor to comply with legal reporting requirements. If an error occurs when using a banknote counter an operator is also able to edit any captured data manually by interfacing with the deposit module GUI.

[0115] Certain customers of the cash processing centre require that deposits are of a certain form. For example, store Y or bank X may stipulate that deposits of 1000 banknotes should comprise a set proportion of different denominations. At steps **535** and **540**, further properties of the banknotes making up the deposit can be captured, possibly using a banknote counter, and compared with the requirements set by the customer. Such requirements may be predetermined or may be stored in data that is accompanies the deposit. If the requirements are not met this can then be logged and flagged to an operator and/or manager. For example, if the denominations of the banknotes of the deposit do not meet the predetermined proportions set by a customer, this may signify that the deposit has been tampered with or is incorrect.

[0116] After the banknotes have been processed at step **535** and the count data has been populated at step **540** the populated count data is compared with the deposit amount entered into the deposit module from the deposit slip. This is performed at step **545**. At this stage, to provide extra security, the result of the comparison may be reviewed by a supervisor at step **550**. If this is the case a supervisor is summoned and logs into the vault management system. Once the supervisor is logged in they are presented with a screen summarising all information relevant to the current deposit. They are then able to review any difference found between the counted amount and the amount on the deposit slip.

[0117] If a difference is found at step **555** then this is displayed to the supervisor and the supervisor is asked to enter a reason for the difference at step **560**. If no difference is found then the supervisor may be asked simply to confirm the count data. Whatever the result, the supervisor then captures an image of the deposit slip at step **565**. This may also be performed by the operator. This typically involves placing the

deposit slip underneath a digital camera connected to client workstation **220**A. The digital camera is adapted to take a picture of the deposit slip and store it with the deposit record in deposit database **215**. After the count has been performed the operator in the deposit processing area **111** the cash is transferred to the vault area **121**. Typically, after processing, the cash is retained in a secure container whose ownership is attributed to the operator, machine or area responsible for deposit processing.

[0118] In certain embodiments, a selective dual control system may be used to implement step **550**. Such a system may also be used at other points within the cash processing cycle where dual control is required, for example, when performing count or reclassification during vault processing **120** or when activating and/or allocating an order to an operator during order processing **130**. The system typically comprises two parallel modules or GUIs that are presented to two different users, wherein processing performed by a first user using a first module or GUI may be approved and/or authorised by a second user using a second module or GUI. If two GUIs are provided these may either be displayed on the same display or on two different displays, wherein the two displays may be provided in the same area or in two different locations.

[0119] In an example wherein a supervisor and an operator use a dual control system implemented using a single display, the dual control system may be initiated by a log-in procedure performed by a supervisor on a client workstation that is presently displaying a first GUI to the operator. Once the supervisor has been successfully authenticated, a second GUI may be displayed together with the first GUI; for example a vertical or horizontal split-screen arrangement could be used. The supervisor may then be presented with data and/or control components unique to his or her level of superiority, e.g. "accept" or "decline" click buttons to authorise count differences as described above. Using a dual screen configuration, the supervisor is able to simultaneously view such data and/or control components together with the options and data of the operator. After completing authorisation a supervisor may log-out of the second GUI, which may act to lock or close the interface.

[0120] The dual control system above may be seen as "selective" as such a system is only implemented when a supervisor logs-in to an appropriate module. Each user within the cash processing system may have associated data that is stored by vault management server **210**. This data may comprise configuration information detailing which executable components or GUIs are available to a user. Thus when a supervisor logs-in, data is exchanged with the vault management server **210** and, depending on the configuration information of the supervisor, the present workstation may be instructed to display the appropriate dual control GUIs. The configuration information may also be used to restrict access to particular modules; for example, an operator assigned to deposit processing **110** may only be able to load modules related to that area of processing and may only be able to see GUIs related to deposit processing operations. The configuration information may be configured by appropriate management personnel.

[0121] The transfer of cash from the deposit area **111** to the vault area **121** involves a transfer process as illustrated in FIGS. **3**A and **3**B. The transfer process is used to transfer responsibility for the cash deposits from deposit processing **110** to vault processing **120**. The transfer process performed by the party wishing to transfer a cash deposit, in this case an operator DP within deposit area **111**, is shown in FIG. **3**A. The operator begins by initiating a transfer module upon client workstation **220**A as shown in step **305**. The operator then selects the source of the transfer in step **310**. The source may be an individual, an area or a safe, a safe being a subdivision of the vault. The selection may be achieved by either selecting the relevant user name or area from a dropdown list, retrieving the current logged in user name or area from the client workstation operating parameters. Once the source of the transfer has been selected the containers and/or cash deposits currently assigned to the source may be displayed to the user via in an information panel within the GUI.

[0122] At step **315** the operator selects a destination, which may also be an individual, an area or a safe, a safe being a subdivision of the vault. For example, the destination may be a user V in the vault area **121**. This selection may again be made through the use of a dropdown menu. Once a user and/or area have been selected as a suitable destination the containers and/or cash deposits belonging to the selected destination may be displayed in an information panel.

[0123] Once the source of the transfer and the destination of the transfer have been selected in steps **310** and **315**, the number of items to transfer is then entered in to the transfer module GUI at step **320**. These items can be containers or discrete bundled quantities of banknotes representing a cash deposit. As discussed previously each container has an identifier and this identifier can be in the form of a barcode. Each bundled quantity of cash may also have an identifier in the form of a barcode. Once the number of items to transfer has been entered at step **320**, the identifiers corresponding to the items that are to be transferred are entered into the transfer module GUI. For example, if barcodes are used these can be scanned at step **325** to obtain serial numbers identifying each item. As each item is identified it may be passed across the physical boundary **141** separating the deposit area **111** from the vault area **121**. Each identified item is counted and the total number of identified items is compared with the quantity entered in step **320**. Once all the items for transfer have been identified then the transfer is confirmed at step **330**.

[0124] In order to complete the transfer process a transfer must be acknowledged by or at the destination. In the present example, this could be operator V in the vault area **121**. An acknowledgement can be performed in one of three ways:

[0125] The system can be set up to automatically acknowledge any transfers as soon as they have been confirmed by the operator at step **330**.

[0126] The receiving party can follow the steps shown in FIG. **3**B. At step **350** the destination operator logs into the vault management system via a client workstation **220** and initiates an acknowledgement module **350**. In certain configurations the acknowledgement module automatically identifies the current user and/or destination area based on the operating parameters of the current client workstation and in other configurations the acknowledgement displays a series of users, areas or safes for the operator to select. Once one of a user, area or safe has been selected the current number of transfers awaiting acknowledgement are displayed. The operator then selects one of these transfers at step **355** and interacts with the GUI of the acknowledgement module to acknowledge the transfer.

[0127] In addition to the steps of FIG. **3**B described above the receiving party may also re-identify the items at step **365** in order to acknowledge the receipt. For

example, the barcodes of two bulk bags received from the deposit area **111** may only be acknowledged when their barcodes are scanned using a barcode scanner **225** connected to a client operating system **220** present in vault area **121**. This option is the most secure and means that items can only be acknowledged once they are physically received.

[0128] This transfer process described above manages the physical responsibility or "ownership" of containers and/or cash deposits. This allows, all physical movements of containers and/or cash deposits between operators and/or areas of the cash processing centre to be recorded by the vault management system as database records. The vault management system running on vault management server **210** stores records of each transfer and each acknowledgement in database **215**. Thus these records can be queried at any time in order to investigate a transfer process. For example, if a transfer has been initiated by one party but the transfer has not been received by a second party then the transfer records for the initiated transfer can be examined and details such as the container identifiers, cash amount, date, time, user and/or area can be retrieved to aid investigation.

[0129] Once the cash is in the vault area **121** it will often be processed and stored. This may involve removing the cash and re-bundling sets of banknotes in set bundles of a particular denomination and a particular fitness. For example, banknotes may be sorted into those that are fit for automatic teller machines (ATMs) or those that comply with the Banknote Recycling Framework (BRF).

[0130] The vault management system further comprises a vault module that allows the physical inventory of the vault or secure area of the cash processing centre to be accurately represented in real time. As all cash deposits are transferred to the vault the vault module is able to calculate the exact quantity of cash within the vault by using the count and denomination records, linked to the transferred item, that were generated during deposit processing **110**. To facilitate management of the vault inventory the vault module further has the ability to generate virtual areas or safes within the vault area **121**. Items such as containers or bundled quantities of cash can then be assigned to specific virtual areas through the transfer process of FIGS. **3**A and **3**B. For example, virtual areas could be generated to hold reserve notes, new notes, coins, ATM fit notes, notes for a particular customer, notes for destruction, old issues of notes, containers, bags, cages, or to represent designated areas such as processing areas or order preparation areas. This can enable management to view all available cash of a given type at a given time, for example all ATM fit cash and then manage the cash flow process accordingly. These virtual areas may have a physical counterpart but this need not be the case, so quantities of cash present in a set physical area of the vault may belong to different virtual areas or safes.

[0131] Vault processing **120** may also involve reclassification of cash media. For example, 100×$1 coins may be reclassified as a 1×$100 rolled coin package. This can help to simplify and refine later order processing. Alternatively, if fitness and authentication sorts are not performed as part of the deposit processing **110** then the resultant quantities of cash will be set as "unclassified". Within vault processing **120** these quantities of cash can be further sorted for fitness and authentication and the results of the sort process can be used to perform the media reclassification. This can enable the true state of the cash or media within the vault to be ascertained. Additionally, by altering the stage at which media classification is performed the processing workload can be actively split between deposit and vault processing.

[0132] Cash remains in the vault area **121** until it is required to fulfil a cash order. FIG. **6** illustrates the steps involved in order processing **130**. A cash order comprises a request for a set quantity of cash from a customer. This request may be for a variety of articles of value, such as coins, notes or bonds and may also include an order for associated servicing, such as ATM servicing. At step **605** the details of the cash order are received or generated. Cash orders may be one off orders or may be part of a regular standing order. Cash orders are stored as records in an order database which may be implemented as part of vault management database **215**. Orders may be received via a variety of communication means, for example facsimile, telephone, email etc, and may be manually or automatically entered into the order database. Orders may also be automatically generated based on forecasting systems that interface with the cash management system.

[0133] Once a cash order is received, an order processing module verifies the customer making the request and checks that the customer is on, or can be assigned to, a valid delivery route. The delivery date of the order is also checked to confirm that it is possible make the delivery and, if the delivery date is not possible, an error is returned. The order amount is checked against the inventory of the vault **121** to confirm that there is enough stock to complete the order. Orders are then queued and grouped by delivery date.

[0134] Before an order can be prepared it needs to be activated and allocated to an operator within the cash processing centre. This is typically performed by a supervisor using a client workstation such as client workstation **220**B within the order processing area **131**. The supervisor logs into an order preparation module, which forms part of the order processing module, and is presented with a list of orders available for preparation. At this stage the supervisor may also make use of any selective dual control system that has been implemented. Commonly, the list is filtered to show a subset of orders, for example those needing to be prepared for the current day, and the supervisor can view the details of each order by selecting one of the list. To activate an order at step **610** the supervisor selects the order from the list and confirms that it is to be activated. At this stage orders can be assigned one of a plurality of types which will dictate any special preparation requirements. Once an order is activated its status is changed to awaiting preparation. This status change is a one way process and activated orders cannot be modified or deleted.

[0135] Once an order has been activated operators within the vault area **121** prepare the cash required to make up the order. At this stage the system may also perform an inventory check. This may involve counting out the amount of cash stipulated in the order. After the cash has been prepared it awaits collection by an operator from the order processing area **131**.

[0136] Meanwhile, after activation of the order, the supervisor proceeds to allocate the cash order to a user and/or an area. Typically, this is an operator within order processing area **131**. To allocate an order at step **620** the supervisor selects an activated order and then selects the required user and/or area in a similar manner to the selection of a destination in the transfer process. It is also possible to allocate more than one cash order. Once an order has been allocated then a pick list or manifest can be printed at step **625**. The pick list contains details of the cash order and may have a barcode

encoding a unique serial number associated with the order. Typically, the pick list is printed by the printing device **240** connected to the client workstation **220**B within the order processing area **131**. The pick list may comprise a number of individual manifests corresponding to each required container.

[0137] Once the responsible operator receives the pick list they are able to retrieve the cash required to make up the order from the vault. This requires a transfer process **630** as shown in FIGS. **3**A and **3**B. The printing of a print list at stage **625** may automatically generate a transfer process to transfer banknotes from the vault area **121** to the order processing area **131**. Alternatively the transfer process can be performed by an operator in the vault area **121** at the request of the order processing operator. In any case, the stages in FIG. **3**A are performed with regard to a number of prepared bundles of banknotes. The operator within the order processing area **131** then receives the banknotes and the transfer process can be acknowledged by the order processing operator as shown in FIG. **3**B.

[0138] At step **635** a number of containers required to hold the cash order are prepared. The number and type of containers required may be calculated automatically when the order is activated and may be present on the pick list. For example, orders can be supplied in cassettes, bulk bags or satchels. The containers are retrieved from a stock of fresh or un-used containers and these may be present in the order processing area **131** or maybe retrieved from the vault area **121**. As with received deposits, each container is typically assigned a unique identifier. This may be encoded as a barcode. The barcode may already be present on the container or the client workstation **220**B within the order processing area **131** may generate and print new barcodes using a connected label printer. Hence, before picking an order the allocated operator is provided with a pick list, a number of identified containers and a quantity of cash from the vault.

[0139] An activated order can only be prepared by an allocated operator. Hence the picking process begins when the allocated operator logs into a client workstation, such as workstation **220**B, in order processing area **131**. The allocated operator is then presented with an order preparation screen. This displays all pending orders that have been allocated to the current operator in an information panel. To perform the picking process at step **640** the allocated operator first selects a pick list and enters the pick list identifier. This may involve scanning the barcode present on the pick list. The entering of the identifier brings up the details of the order on the operator's screen. These details include the number of containers required and the amount of cash or number of banknotes to be placed in each container. The operator begins with a first order container and enters the container identifier associated with the first order container. This may involve scanning a barcode related to that container. The operator is then informed of the quantity of cash to be placed within the container. If the cash is in the form of bundled banknotes a number of bundles can be taken and placed into the container to pick the order. If the cash is provided in the form of a heterogeneous group of banknotes or other documents then the cash may be counted by an attached banknote counter, such as counter **230**C. If said counter is connected to the client workstation then the order processing module may automatically pass the required count amount to the counter. The operator then need only place a quantity of banknotes upon the counter and the required amount will be counted into an appropriate output hopper. The operator can then simply remove the banknotes from the output hopper and place them in the associated container. If each container has its own manifest or the order is complete, the appropriate pick list is placed within the container and the container is then sealed. The pick process is then repeated for any additional containers that make up the order.

[0140] After the picking process a balance is calculated for the user based on a comparison of the quantity of cash received from the vault with the quantity of cash placed within the one or more containers. These quantities should be equal and if they are not then a supervisor can be called over to log in and confirm the reason for this difference. If an error occurs during the picking process then picked quantities of cash can be retrieved from assigned containers but the associated container identity is destroyed and a new container identity is generated. The end result of the order processing process **130** is one or more containers filled with a quantity of cash that fulfils a given customer order.

[0141] FIG. **1**B illustrates an extended cash management process **101** according to a second embodiment of the present invention. This process **101** provides an extension to the cash management process **100** shown in FIG. **1**A. The extended cash management process **101** further comprises the processes of cash reception **150** and cash despatch **160**. The incoming delivery of cash deposits and the outgoing despatch of cash orders may be performed by the same organisation that runs the cash processing centre or may be performed by a third party. Although the present example is described with the inclusion of the reception **150** and despatch **160** stages it should be noted that these stages are optional and the present invention can be implemented using any of the stages shown in FIG. **1**A.

[0142] FIG. **1**D illustrates an example schematic of an extended cash processing centre **106** according to the second embodiment of the present invention. Extended cash processing centre **106** comprises deposit processing area **111**, vault area **121**, and order processing area **131**, as present in the standard cash processing centre **105** of FIG. **1**C, but also further comprises reception area **151** and despatch area **161**. Reception area **151** may be separated from the deposit area **111** by physical boundary **171** as shown in FIG. **1**D. If so, access to the deposit area **111** from the reception area **151** is provided by entry point **156**, through which cash can be transferred as shown by arrow **157**. Alternatively, the reception and deposit areas may be provided by a single area. Despatch area **161** may also be separated from order processing area **131** by physical boundary **171**. If so, access to the despatch area **161** from the order processing area **131** is provided by exit point **136**, through which cash can be transferred as shown by arrow **137**.

[0143] FIG. **1**E shows an alternate layout for a cash processing centre, wherein features equivalent to those shown in FIGS. **1**C and **1**D are given identical reference numerals. Delivery bays **151** and **161** are used as reception and despatch areas, wherein delivery vehicles may reverse into said bays to load and unload cash deliveries. Deposit area **111** comprises two areas: area **111**A comprising desk-top machines similar to workstation **220**A and area **111**B comprising large banknote sorters and a reject entry station. Selected deposits and rejected notes will pass from area **111**A to area **111**B through entry way **181**. Vault **121** is located in the centre of the cash processing facility and receives cash from area **111**A via route **117** and area **111**B via route **182**. Order processing area

131 receives cash from the vault 121 and picks orders to supply to the despatch area 161.

[0144] Cash reception 150 involves the receipt of containers that contain cash for deposit. Commonly, these containers are received from CIT operators which transport cash deposits from parties who are located at a distance from the cash processing centre. For example, at the end of a trading period, a bank may commission a CIT operator to pick-up cash from the bank's branch and transport it to the cash processing centre. During cash reception 150 the cash processing centre is responsible for unloading containers containing cash deposits from a CIT vehicle and documenting the newly acquired ownership of these containers.

[0145] Responsibility for these containers can then be transferred to deposit processing 110. In a similar manner to the boundary line 140 in FIG. 1A, the extended cash management process 101 of FIG. 1B contains figurative boundary line 170. This separates the process of cash reception 150 from the process of deposit processing 110 and reflects the organisation of the discrete components of the vault management system.

[0146] An example of the cash reception process 150 is shown in FIG. 4. The method 400 shown in FIG. 4 is implemented when a cash deposit is received at the reception area 151. For example, the method may be initiated when a CIT vehicle arrives. As with deposit and order processing, the cash reception process is performed by an operator resident in reception area 151. The operator has access to an additional client workstation within the reception area 151. On arrival of a cash deposit, if an operator is not already logged in, the operator loads a cash reception module and logs into the system using their user name and password.

[0147] The operator then proceeds to capture data associated with the cash deposit. This begins with the step of entering the carrier or the route details 405 into the vault management system. Typically, this involves entering a carrier or route identifier from CIT or deposit documentation. This identifier can either be entered manually by the operator or automatically by scanning a barcode encoding the identifier.

[0148] At the next stage 410 deposit information related to the received cash is entered into the vault management system. This may comprise the number of containers being deposited or may comprise additional details such as the name of the depositing customer and/or the deposit amount. In a similar manner to the entry of the carrier or route details 405 the deposit information may be entered manually by the operator or may be retrieved from data encoded into the CIT or deposit documentation. At the next stage of the method the identifiers of the received containers containing the cash deposit are entered into the system. Typically, each container has an external barcode encoding the container identifier and this is scanned using a handheld barcode scanner in step 415. The cash reception module then stores the identifiers of each container and verifies that the number of containers present in the CIT or deposit documentation matches the number of identified containers.

[0149] Once all the received containers have been identified to the system then reception of the deposit is confirmed at step 420. This can be achieved by pressing an icon within a GUI used to implement the cash reception module. On receipt of a new cash deposit a number of new deposit records are created in the vault management database 215. Each container will have its own associated record which will contain information about its source, its contents and other processing information. When the reception of the cash deposit is confirmed at the confirmation stage 420 these records are permanently stored in the vault management software database 215 and the containers are assigned or allocated to the current operator and/or area. At this stage, "parent" containers containing one or more other containers may be unloaded or loaded to facilitate deposit processing. The opening and loading of a container in this or in related operations may be provided as a single option within the module. Before transfer to the deposit processing area 111 a reception operator is also able to re-load the reception module and edit any incorrect data.

[0150] Once a number of containers containing cash deposits have been received and documented in reception area 151 the containers are transferred to deposit processing area 111. Physically this is normally achieved using entry point 156. As well as physically transferring containers of cash between area 151 and 111 the reception operator must also complete a transfer process. As before, this transfer process is required to record the movement of the cash deposit containers. Hence the reception operator performs the steps of FIG. 3A whilst an operator in the deposit processing area 111 acknowledges the transfer, for example using the steps of FIG. 3B. Deposit processing can then begin as described with relation to FIGS. 5A and 5B.

[0151] The deposit information captured at step 410 may be stored as initial data in the appropriate deposit record in vault management database 215. This data may then be used again in a later stage of processing to save time. For example, the deposit information may comprise a customer name or identifier and a deposit amount. During deposit processing 110 this initial data may be retrieved and used to initially populate fields within the deposit processing module. The operator performing the deposit processing 110 may then have the opportunity to confirm this initial data, for example verify the customer identifier and details and the cash amount on the deposit slip. If there is a high level of trust within the system the initial data may be confirmed automatically.

[0152] The extended cash management process 101 of FIG. 1B also includes a despatch stage 160. After an order of cash has been processed by the order processing stage 130 it is typically sent to the despatch stage 160 to be despatched to the customer requiring the cash. The delivery is normally performed by a CIT operator. The despatch stage also records the transfer of responsibility from the cash processing centre to the party responsible for the delivery. The steps performed during cash despatch are shown in FIG. 7.

[0153] The result of the order processing stage 130 is a number of containers containing a quantity of cash to fulfil a cash order. Once an order has been prepared and processed it is transferred to the despatch area 161 to await despatch. Physically, this is often performed using a secure exit point 136. As part of the management process the one or more containers that contain the cash required for the cash order are also transferred to the despatch area 161 using a transfer process 135 as described previously with relation to FIGS. 3A and 3B. The transfer process is initiated by an operator within the order processing area 131 and a second operator logged into a client workstation within despatch area 161 acknowledges the transfer as well as physically receiving the containers.

[0154] Once in the despatch area 161 the operator may combine a number of cash orders into a shipment, as is shown in step 705 of FIG. 7. A shipment corresponds to a plurality of

customer orders that will use a common despatch route or CIT operator. Alternatively, orders may be grouped into a shipment by management personnel or automatically based on scheduling considerations. In any case, when the despatch operator logs into the vault management system and loads a shipment module they are presented with a screen displaying all shipments scheduled for the present day. The shipment module may also display whether all containers for a given shipment are available for despatch or whether a shipment is incomplete or over-subscribed. Containers for a given shipment may be prepared in step **710** by physically grouping the shipment containers in a reserved section of the despatch area **161**. Each shipment may have an associated printed manifest documenting the details of the shipment.

[0155] When the appropriate transport vehicle arrives at the cash processing centre the despatch operator begins the despatch process. The operator begins by loading the despatch module on a client workstation and selecting the route used by the waiting transport vehicle. The despatch operator then enters or selects the relevant shipments for that route and enters the number of containers to load onto the vehicle for each shipment at step **720**. This may be achieved by scanning the barcode of a shipment manifest to retrieve a shipment identifier. The identifiers of all the containers to be despatched are entered into the despatch module which assigns these containers to the operator of the transport vehicle. This may be achieved by scanning container barcodes that encode a unique container serial number, as is set out in step **725**. The identification of the containers making up the shipment transfers ownership of the containers from the despatch area **161** to transport vehicle operator. The order containers are then physically loaded onto the transport vehicle in step **730**. A manifest related to the shipment and documenting the transferred containers may be generated in step **735**. This manifest may be printed onto paper or may be stored electronically. The transport vehicle is then ready to depart the cash processing centre with the loaded containers.

[0156] As the steps in reception and despatch processing typically involve working with CIT or other delivery or despatch vehicles it is advantageous if operators within these areas are provided with portable electronic devices to perform the steps of FIGS. **4** and **7**. For example, an Ultra Mobile Personal Computer (UMPC) or PDA, together with an optional touch-screen input, may display the required forms to an operator located within areas **151** and **161** as shown in FIG. **1**D. Selection and manipulation of user interface controls by the operator may then provide the data input and/or confirmation required in the steps of FIGS. **4** and **7**. The UMPC or PDA may optionally be equipped with a barcode or RFID reader to automatically obtain data from deposit or despatch containers (see the description below for further details of RFID integration). The UMPC or PDA may also be adapted to receive signatures from CIT or other delivery personnel, for example using a stylus and a touch screen interface. Hence, deposits and cash orders may be digitally "signed for" to confirm the transfer of cash to and/or from said personnel.

[0157] A third embodiment of the present invention is shown in FIG. **8**. This embodiment combines the vault management system of the first or second embodiment with a closed-circuit television (CCTV) system; the embodiment comprises the hardware components of FIG. **2**A but then further comprises CCTV cameras **820** and a CCTV multiplexer and recorder **810**. Typically cameras **820** are digital CCTV cameras and CCTV multiplexer and recorder **810** is adapted to store digitally recorded CCTV footage in database **815**. Digital CCTV systems capture a video using high-capacity, high-speed multi-channel digital recorders. Such systems typically hold a vast amount of video footage and allow quick access to video files stored in database **815**.

[0158] Using the assignment of containers and assets, together with the transfer process, the vault management system of the first and second embodiments is able to capture data related to all cash processing actions in its database. Each recorded action, for example a transfer, count or reception operation, will have an associated date, time and location. In a similar manner the CCTV system will monitor set locations and will index each video recording using a date and a time. Hence, as both the vault management system and the CCTV system are commonly linked by location, date and time parameters it is possible to retrieve video footage from database **815** based on a location, date and time specified by the vault management server **210**.

[0159] For example, a supervisor may wish to view the transfer of a set of containers between the order processing area **131** and the despatch area **161**. Such a transfer will have an associated transfer record in the vault management database **215**. This transfer record will then comprise data specifying an associated set of locations (areas **131**, **136** and **161**) and an associated date and time. The vault management server **210** is then adapted to supply these parameters to the CCTV multiplex and recorder **810** which is able to retrieve the appropriate video from video database **815**. The supervisor is then able to view the video footage for that location, date and time. If the CCTV camera is positioned to monitor the display of a particular client workstation, that workstation may be configured to use large fonts that can be accurately read in CCTV footage.

[0160] In certain embodiments, data pertaining to transfer or transaction records generated by the vault management server **210** may be transmitted in real-time or at predetermined intervals to the CCTV system (i.e. devices **810** and **815**). The CCTV system may then use such data to annotate video records stored in video database **815**. For example, data such as the data or time of a transfer, count or other processing operation being performed in a particular area of the cash processing centre may be stored with the video records of said area. In certain embodiments this data may be in the form of text that is added in real-time as an overlay to video footage, for example as a "ticker-tape" that repeats in a rectilinear section at the bottom of each frame of the video footage. In these embodiments the video footage, together with added visual information relating to the vault management records, is stored in a chosen format, such as one of the Moving Picture Experts Group (MPEG) formats, in database **815**. The video footage can then be retrieved at a later date for viewing together with the added visual information. In other embodiments, data relating to the vault management system may be embedded into the video footage without being visible in said footage. For example, data could be incorporated into header sections or unused bits. An appropriate decoder is then able to extract and display the data when the video footage is retrieved. An example of relevant information that is stored with video footage is a list of discrepancies in cash processing operations in a particular area at a particular time.

[0161] As well as integrating the vault management data with a CCTV system other supervisor functions may also be optionally integrated to facilitate management of the cash

processing centre. The supervisor functions described herein may be used with any embodiment of the present invention. The interfaces for these supervisor functions can be viewed using a remote client workstation such as workstation **220**C. The first of these modules is an investigation and research module. This provides a front-end to the vault management database enabling the supervisor to query and view all deposit transactions, all transfer processes and all inventories across any networked cash processing centres, including user and/or area inventories. Each query or inventory may also be printed as an electronic or paper report. Reports include, amongst others, operator productivity, discrepancy pattern analysis, deposit quality per depositor, counterfeit frequency per depositor or ATM fit note yield per depositor. These reports may be generated automatically when certain criteria are met, for example at a particular time every day, week or month. Such scheduling may also be combined with technologies to automatically distribute or publish the reports; for example, a scheduled report may be faxed or emailed to a particular group of users. Discrepancies reported by customers can be investigated by recalling all data associated with the deposit and/or cash order in question, including the image of the deposit slip. Discrepancy reports can then be generated and printed or sent electronically.

[0162] As a variation of the reporting described above, the vault management server **210** may be adapted to provide ad-hoc text output files. These files are configurable; operators and management may select which fields from vault management database **215** they wish to export into a text file and these selections may be altered in real-time. For example, a manager may wish to regularly export performance metrics relating to the cash processing centre into an XML file for publication on an internal or external server. The vault management server **210** may also be adapted to process and import data, such as data relating to received orders.

[0163] The vault management server **210** may also be configured to manage alerts, alarms and notifications to employees and/or management personnel (often referred to as "Nagware" in the art). For example, an operator may require a supervisor to authorise a discrepancy or shortfall in a required cash amount. In the past, the operator typically raised their hand and waited to be noticed by a supervisor. This process was inefficient and required a supervisor to monitor the whole of a department at any one time. The vault management system **200** of the present invention may be configured to automatically detect events that require authorisation. Such events may be detected when an operator reaches a certain point in a process or workflow or when a particular set of data exists. Once an event is detected it may initiate a routine to alert a supervisor. This alert may be provided by, amongst others, one or more of: short message service (SMS) alerts to a cellular mobile phone, paging alerts over amplitude or frequency modulation (AM or FM) frequencies to a pager, or "pop-up" windows that are activated upon a supervisor workstation, such as **220**C. The alert may contain, amongst others, one or more of: the operator needing assistance, their location, the time of the alert, its urgency, the level of management required, and the alert category. The system may also be provided with a time-out mechanism; if the required supervisor does not attend to the alert within a configurable period the alert may be logged or another member of staff may be alerted, possibly in the next level of management hierarchy. Such alerts may also be used for service management.

[0164] In some configurations it is also possible to provide keystroke and/or device logging that can provide an extra level of information for audits or investigations. For example, all key-strokes and control selections performed by a user during a transfer or transaction may be monitored. Hence, if an operator takes 100 euros from a cash deposit and subsequently cancels an alert showing a 100 euro discrepancy, both the alert and the cancelling of the alert will have been recorded by the logging system and may be used as evidence of theft. The logging may further be synchronised with the CCTV system of FIG. **8**. For example, the date, time and location of each keystroke or operation may be stored in a database. If a supervisor is concerned about a particular sequence of keystrokes, the associated CCTV footage may be retrieved as described above.

[0165] A security console may also be provided to inform a manager or supervisor of any potential security risk within the cash processing centre. The security console may comprise one or more GUI indicators. These GUI indicators may be graphical and/or text-based. For example, in one particular embodiment each indicator may comprise a dial resembling those found within a motor-vehicle dashboard. Each dial may display the value of a key performance indicator (KPI) and different areas of the dial may be given different colours. For example, if the KPI ranges from 0 to 10 and a sub-range of 7 to 10 represent a high security risk, a circular sector of the dial representing this sub-range may be red; likewise a circular sector of the dial representing the sub-range of 4 to 6 may be amber. Each KPI may be calculated using a custom formula or algorithm applied to the vault management data. For example, the KPIs may comprise, amongst others, any one of: the number of counts for a particular user performing cash processing operations in any one of areas **110**, **120**, **130**, **150** or **160** of for a particular delivery route in which the cash amount falls short of a previously recorded amount, the number of transaction adjustments, the number of counterfeit notes detected per machine operator, etc. Security personnel monitoring the security console can thus be provided with clear feedback of the present security situation. The security console may also be integrated with the CCTV system so video footage of events related to each KPI may be retrieved and viewed using the appropriate time-stamps of said events.

[0166] The security console methods described above may also be extended to display KPIs associated with the functionality of database **215** or of a particular banknote counter or processing device. For example, database health or performance metrics such as hit ratios and reads per time period may be displayed using "dashboard" displays or machine processing metrics may be displayed on screens in proximity to the banknote counter or processing device. Alternatively, one or more KPIs may be defined by customers or management of the cash processing centre. Typically, such KPIs are implemented by performing a query on database **215**, wherein the results are updated in real-time. time. For example, bank X may require that all cash deposits are processed by 3 pm. Personnel within the cash centre may then be shown an indicator illustrated how many cash deposits for bank X have yet to be processed, together with the estimated completion time based on the average processing time per deposit. Personnel of all levels are then aware of whether the target is going to be met and can adjust their behaviour accordingly.

[0167] A supervisor may also be provided with a stock balancing function that can be used to balance stock at the end

of a working day or shift. The exact time or event that triggers a balance procedure is configurable. An operator first uses the system and logs into the balance module. They then select their name from a list onscreen and are presented with a list of the stock that is currently assigned to them. The operator then performs a count of the cash within their work area and enters the count result into the module. This process may also be performed without displaying the expected stock to perform the balancing "blind". If a difference is found between the expected and actual stock count the module will prompt the operator to perform a recount. If after the recount an imbalance still remains a supervisor is summoned. The supervisor is then able to adjust the balance if need be or investigate any discrepancy.

[0168] The balancing procedure described above may be performed using a technique referred to as High Speed Teller Balancing (HSTB). This technique uses the methods described below with reference to FIGS. **9**, **10** and **11**. The banknotes that have been processed by one or more operators may be collated into a number of note bundles separated with header and/or trailer cards. The note bundles are then processed by a high-speed, high-throughput banknote counter, such as that shown in FIG. **10**, and the data generated by such processing is reconciled with the data produced by each operator using a smaller banknote counter or sorter. Any discrepancies may then be identified and investigated. This process can be performed based on count data, i.e. the number of notes in a particular bundle processed by the high-speed counter match the number of notes previously processed by a particular operator, together with any number of optional variables such as denomination or authenticity.

[0169] As well as the examples discussed above, any of the ownership, count, sort, inventory, reclassification and order processing data can be used together with other relevant collected data to provide a real time summary of key performance indicators (KPIs). These may be displayed visually to a supervisor or an operator. Any known data processing used in the art may be applied to the data to provide appropriate management information to a wide variety of personnel, from senior management to low-level operators.

[0170] The vault management server **210** may also be adapted to manage user or operator accounts. Typically, each employee associated with the cash processing centre has a user account which they use to log-in to the vault management system **200**. Log-in or authentication may be performed through modules of the vault management system **200** implemented by one of the client workstations **220** or directly with the vault management server **210**, for example through a web-based interface. Each log-in procedure may involve exchanging data such as a user name and password with the vault management server **210**. The vault management server **210** may then authenticate this data against data stored in the user account and, if the log-in request is approved, appropriately configure future processes. The user data may be stored in a database operably connected to the vault management server **210**, which may be database **215**.

[0171] The user account may store a variety of data. For example, the user account may store data indicate which commands, GUIs or processing modules a user has access to. For example, a deposit processing operator may be limited to accessing a deposit processing GUI or module and may not have the option to load or access an order processing GUI or module. This data may be configurable. For example, management may wish to assign an operator from deposit processing **110** to order processing **130** and thus may wish to appropriately change the access permissions of the operator. Additionally, users who are higher in the management hierarchy may have access to a greater number of GUIs or modules.

[0172] The vault management system **200** may also be configured to automatically log-out a user or lock their system if their workstation or module is idle for a predetermined period of time. If this occurs the user may have to log-in to the system a second time to reactivate any idle processes. This may increase security and prevent unauthorised access. The period between the last action and the locking and/or the log-out procedure may be configurable according to user or user group. The system may also be configured to "roll-back" any pending transfer or transaction that is interrupted by the locking or log-out procedure. More details of "roll-back" operations are given below. As a user may have a plurality of executable modules loaded upon a client workstation the locking and/or log-out procedure may be applied to one or more of: the client workstation, one or more active modules, and all modules loaded upon the workstation. For example, the system may log a user out of any background processes that have not been activated in the last five minutes.

[0173] In one embodiment of the present invention, user accounts for a selected plurality of users may be assigned to a user group. For example, operators performing vault processing **120** may be assigned to a vault processing group. Data that is common to all users within the user group, for example permission data, shortfall amounts that require authorisation or available GUIs, may be stored as metadata for the user group. The vault management server **210** may then be adapted to use this metadata as user account data for all users within the group. For example, for the vault processing group, the metadata may comprise a field indicating that all shortfalls in count amount above 5 euros require authorisation by a supervisor. In use of a vault processing module, said module may make use of this field to decide when to lock the module and request supervisor authorisation. Due to inflation, management may wish to increase the 5-euro limit to 10 euros. Instead of having to individually edit the user account data of each operator performing vault processing **120**, management may simply edit the metadata for the vault processing group, i.e. instead of having to edit the shortfall field for every operator, management only needs to edit a single shortfall field in the metadata.

[0174] The vault management server **210** typically offers the option to add, edit or delete a user account for a particular user or a user account group for a particular group of users. For example, a user may be allowed to edit their password and/or user name. Within the vault management system **200** there is the constraint that, when an employee has left the cash processing centre, the associated user account must be maintained to view and manipulate historical data stored in database **215**. For example, each deposit transaction, transfer process and inventory recorded by the vault management system **200** is commonly associated with a particular user. Even if the user has now left the cash processing centre, management may wish to retrieve an audit trail of all transactions associated with the user, for example, as part of a criminal investigation. However, maintaining unused user accounts places a burden on management staff, as they need to select and monitor current employees. The present invention offers a solution to this problem by adding a field to each user account or user account group to enable the logical

deletion of a user whilst maintaining the physical data associated with the user account or user account group. For example, each user account or user account group may have a binary flag that indicates if the user is active. This flag may be set by selectively activating a "Disabled" tick-box in a user-account configuration GUI. Once the tick-box is checked the vault management server **210** is configured to appropriately filter the user accounts to exclude unused user accounts from lists of current users.

[0175] The teachings above in relation to user accounts and user account groups may also be applied mutatis mutandis to customer accounts. Such customers may be those who deposit cash or who receive outgoing cash orders.

[0176] The vault management system **200** and/or database **215** may be provided with a "roll back" function to enable changes to the system and/or database performed within a particular time period to be removed. This has the effect of returning the system and/or database to a previous state. This may be applied at the level of software updates or single transfers and transactions using database methods known in the art.

[0177] A fourth embodiment of the present invention is illustrated in FIGS. **2**B, and **9** to **11**. This embodiment provides an alternative method for performing deposit processing **110** that is adapted to handle large quantities of cash.

[0178] FIG. **2**B illustrates a suite of exemplary hardware components that may be used to implement the fourth embodiment of the present invention. Such hardware as described below may also be used to implement any of the other embodiments of the present invention described herein. FIG. **2**B shows two networks **231**A and **231**B that communicate with each other and a remote client workstation **220**C using WAN **245**. Each network **231**A and **231**B is connected to a respective router **235**C and **235**D which then provides the gateway to the WAN. Remote client workstation **220**C is connected to a third router **235**E via firewall **250**. Each network **231**A and **231**B may correspond to two different areas of a cash processing centre, for example deposit area **111** and order processing area **131**, or to two physically separate cash processing centres belonging to a single organisation.

[0179] Top network **231**A is connected to vault management server **210** and mirror or RAID (Redundant Array of Independent Disks) server **211** which together run the server operations of the vault management software and include a vault management database (not shown). Lower network **231**B interfaces with vault management server **210** via the WAN **245**. Both networks further comprise uninterruptible power supplies (UPS) **255**A and **255**B, reports printers **240**, client workstations **220**A and connected handheld barcode scanners **225** and currency sorting machines **260**D and **260**E. An exemplary currency sorting machine **260** is illustrated in FIG. **11**. The machine **260** comprises document feed area **1012** and document output hoppers **1014**. The document output hoppers further comprise reject hopper **1014**R. While the fourth embodiment is described with regard to the hardware configuration of FIG. **2**B it is not limited to such a configuration and can be used with any other suitable configuration including that of FIG. **2**A. In the latter case banknote counter **230**A is replaced by currency sorting machine **260**.

[0180] Multiple cash processing centres may record data such as ownership transfers, count data and inventory information on a single central database server. This central database server may comprise a primary and back-up server and be accessible from each cash processing centre over a WAN. The database server may also be accessible from a central administrative head-quarters or office.

[0181] The database server may also provide some or all of the functionality of vault management server **210** and may be connected to a network resembling network **231**A but without the cash processing centre workstations **220** and banknote counters **260**. Standard firewall technology can be implemented so that networked machines within a cash processing centre can only see data upon the database server that relates to the centre in question. However, administrative machines may be able to access, view and aggregate data from a plurality of cash processing sites.

[0182] The method of the fourth embodiment illustrated in FIG. **9** provides an alternate method for performing deposit processing as illustrated in FIGS. **5**A and **5**B. In the first and second embodiments each deposit is commenced, counted, validated and completed prior to moving onto the next deposit. The cash pertaining to such a deposit typically remains with a deposit operator at all times. In the fourth embodiment a plurality of deposits are batched together and processed in a continuous cycle away from the desk of an operator.

[0183] The method of deposit processing according to the fourth embodiment involves three main stages: preparation; note sorting and deposit counting; and reject entry. Reject entry comprises capturing data related to notes that were rejected within the sort process. Such notes may be damaged or counterfeit.

[0184] The method **900** of FIG. **9** commences after an operator within the deposit processing area **111** receives one or more containers containing a cash deposit. The operator performs the steps of FIG. **5**A as per the first embodiment but at step **520**, when the deposit record is updated, the deposit is assigned a unique deposit identifier as shown in step **905**. This deposit identifier allows the deposit to be tracked for the duration of the deposit processing. For large deposits the deposit may be split into a plurality of smaller deposits which will each be assigned a unique deposit identifier. Once the deposit identifier has been assigned a set of two separator documents are generated at step **910**. The deposit is then arranged in a deposit batch in step **915**.

[0185] A series of three deposits and their associated separator documents **1112** that make up an exemplary deposit batch are shown in FIG. **11**. The separator documents are designed to be placed around a bundle of banknotes **1116**, **1120**, **1124** making up the deposit and comprise a "first" or downstream document, **1119**, **1121** and **1123**, and a "second" or upstream document, **1118**, **1122** and **1126**, wherein the banknotes are configured to be fed in the direction of arrow **1127**. The first separator documents **1119**, **1121** and **1123** act as a trailer and the second separator documents **1118**, **1122** and **1126**, act as a header. Each header document comprises one or more magnetic strips on the rear (downstream) side of the document and a barcode on the front (upstream) side of the document. The unique deposit identifier is typically encoded in both the barcode and the magnetic strip.

[0186] Alternatively, the separator documents may be taken from a stock of pre-existing separator documents. In this case, each the barcode and magnetic strip(s) encode an arbitrary serial number. This serial number is then assigned to a deposit at step **905** by scanning the barcode on each header document whilst putting together the deposit batches.

[0187] Each deposit batch is commonly arranged on a deposit tray that is adapted to feed a currency sorting machine

260. A deposit batch may contain a plurality of deposits from difference customers. Once a deposit tray is full, or a deposit batch reaches a predefined size, it is taken by an operator to the currency sorting machine **260** for processing and counting at step **920**. The deposit batches, complete with separator documents, are placed onto a feed mechanism of the currency sorting machine **260** at feed area **1012** and the machine continuously feeds the note into a note processing area. The processing performed by the currency sorting machine **260** incorporates one or more of counting, authentication, fitness and denominational sorting in a single process run and typically provides all four forms of processing. During the sort process detectors within the machine inspect both the banknotes and separator documents. When the machine encounters a header document it reads the unique identifier on the document encoded in either the magnetic strips or the barcode. This identifier is then associated with the sort or process records of the subsequent banknotes. When the trailer separation document is then subsequently detected the machine then disassociates the unique identifier from the sort or process records of subsequent banknotes.

[0188] Sorted banknotes are provided to output hoppers **1014** depending on the sort process. For example, a detector may be provided for determining the denomination of each banknote and another detector for determining authenticity. If a banknote is found to be authentic and its denomination can be determined, it will be directed to a particular output hopper for stacking genuine banknotes with that denomination. All other documents either non-genuine or unreadable banknotes or separators are fed to the reject hopper **1014**R.

[0189] The processing data associated with a deposit amount originally situated between the separator documents is sent by the currency sorting machine **260** via network **231**A to vault management server **210**. The server then populates the deposit count and processing data at step **925** using the unique deposit identifier as an index.

[0190] Reject banknotes fed to the reject hopper **1014**R remain sandwiched between their associated separator documents and form reject deposit batches. These reject deposit batches are then taken to a reject processing station wherein the reject notes are processed a second time at stage **930** to ascertain the reason for rejection and/or possible detect good notes that were not detected on the first pass (for example if they were rejected as overlapping or misfed notes). The reject data is also associated with the unique identifier on the header document and is sent to the vault management server to update the deposit count and processing data. Alternatively, the reject notes can be manually inspected by an operator. In this case the operator will manually scan the barcode on the associated header document and enter the reject data.

[0191] Once process data for all the banknotes within the deposit has been ascertained then this data is automatically reconciled with data obtained from the deposit slip at step **935**. As with the first embodiment any discrepancies are flagged to a supervisor in a management report produced at step **940**.

[0192] The benefits of the fourth embodiment are numerous. The deposit processing is performed in one continuous process and a high level of accuracy, integrity and security is maintained. Added security can be provided by performing the processing "blind", i.e. the operator responsible for operating the counter and/or entering reject information is unaware of the depositor details.

[0193] A fifth embodiment of the present invention is illustrated in the flowchart of FIG. **12**. This embodiment incorporates customer processing of cash deposits before said deposits are delivered to the cash processing centre, commonly referred to as "pre-advisement". The "pre-advisement" method discussed below preferably uses radio frequency identification (RFID) devices in order to facilitate data management during the cash deposit process; however, the method can equally be applied within the RFID functionality, with the loss of certain advantages. Reference to a customer refers to a customer of the cash processing centre.

[0194] In the flowchart of FIG. **12**, steps **1265** are performed by the customer or organization making a deposit. As such, these steps may be performed upon the customer's premises or within their place of business, for example within a back office in a retail environment. At step **1205**, the customer prepares a new cash deposit. This deposit will typically comprise a quantity of cash, cheques and/or documents of value that the customer wishes to deposit at the cash processing centre. The length and complexity of this step will depend upon the size and nature of the customer and/or organization. For example, in a large retail organization, a customer may move their till takings from the front of the shop to the back office after closing, wherein the takings will be counted and sorted to produce a deposit for that day of trade. During the preparation of this deposit a deposit reference is typically generated at step **1255** which allows the customer, and subsequently the cash processing centre, to identify the deposit. In certain embodiments the deposit reference may be an alpha-numeric code. The deposit reference may be generated automatically at the end of trade or maybe actively generated by the customer upon preparing a new cash deposit. For example, a user may select a new deposit action from a user interface present upon deposit management software running on a computer terminal in the retailer's back office.

[0195] The customer will then prepare the cash and/or articles of value for deposit. This typically comprises sorting the articles for deposit into bundles of banknotes of a certain cash value or of a number of banknotes of a set denomination. This sorting may be performed in conjunction with a banknote sorter present upon the retailer's premises. For each bundle deposit generated by the retailer, the customer attaches one or more separator documents. These separator documents may comprise the header and trailer cards **1118** and **1119** shown in FIG. **11**. Two of these separator documents are placed around the bundle: a header card **1118** on the top of the bundle and a trailer card **1119** on the bottom of the bundle. These separator documents may comprise plastic cards for durability, and be designed to be hard-wearing.

[0196] In the present case, the header card **1119**, forming part of the separator documents attached to a bundle of banknotes, comprises a barcode and an RFID or wireless electronic chip. As each bundle is formed, such as bundles **1116**, **1120** or **1124** in FIG. **11**, the retailer will scan the barcode present on the header card associated with each bundle. This barcode will typically encode an identifying serial number or alpha-numeric code. This number or code is then associated with the deposit reference calculated in step **1255** and step **1260**.

[0197] The RFID chip typically comprises an integrated circuit and an antenna and may be similar to the chip shown in FIG. **14** and described in the section on RFID Tracking below. The antenna is used for receiving and transmitting a wireless or radio frequency signal and the integrated circuit is typically

used for storing an identifying serial number or alpha-numeric code and for modulating and demodulating the wireless radio frequency signal. On supply to the customer the RFID chip is set to typically read-only. In a variation of step **1210**, the customer may alternatively prepare the bundle and then instead of scanning the header barcode, pass the bundle under a RFID reader which will communicate with the RFID chip and retrieve the identifying serial number stored in the chip. This number is then associated with the deposit at step **1260**. The association is typically performed by storing the retrieved serial number and the deposit reference in a central database. This central database may be coupled to a web server accessible by both the customer and the cash processing centre over a WAN or may be database **215**. Alternatively, the association may be stored in a local database at the customer's premises and then sent to the cash processing centre by electronic communication. In certain embodiments, both the barcode serial number and the RFID serial number may be stored with the deposit reference. The RFID chip may also be located in a different separator document to that which contains the barcode.

[0198] In alternate embodiments that do not use an RFID chip, the customer or retailer may print their own header cards **1119**. For example, at step **1255**, on creation of a new deposit and the generation of a new deposit identifier, the customer may be given an option to print one or more header cards containing the deposit identifier. A header card **1119** may be printed onto adhesive labels, paper, card or plastic (amongst others) and the deposit identifier may be incorporated into the header card in the form of a one or two dimensional barcode. This provides a cheap method of providing customers with header cards and enables the header cards to be disposed of, preferably recycled, after use.

[0199] During the preparation of the cash deposit at step **1205**, the customer will generate deposit information relating to each bundle. For example, this may be at least one of: date and time of processing, personnel present, location of processing, count information, the total value of the bundle, the number of notes of a particular denomination, authenticity information related to the notes within the bundle and fitness information such as the level of soil or tears. This deposit data may either be produced by hand, based on a manual count, and individual inspection of each note within the bundle, or may be produced automatically using a banknote sorter. If the information is produced by hand it may be recorded against the bundle RFID and/or barcode reference using a user interface displayed on a customer computer terminal. If the information is produced by the banknote counter it may be passed in electronic form to the customer's computer for storage against the bundle RFID and/or barcode reference (and thus in turn the deposit reference) or maybe displayed to the customer for manual entry against the bundle reference using a user interface. This allows a running total of the current deposit to be calculated after processing each bundle.

[0200] The banknote sorter may be further adapted to take a plurality of banknotes and/or articles of value as input and produce a number of banknote bundles with pre-determined properties as output. For example, the banknote sorter may automatically produce bundles of one hundred notes of each denomination, for example one hundred notes of 10 dollar or 10 euro value and then automatically place a header and trailer card around the bundle before the bundle is output to a sorter output tray or stack. The banknote sorter can then be adapted to read either the barcode or the RFID chip serial number as the bundle is put together to automatically associate the separator card or chip identifier with the processing details of the banknote bundle.

[0201] At step **1215**, the produced cash bundles are placed into one or more containers ready for transportation to the cash processing centre. Each container may optionally also comprise a barcode and/or RFID chip, in which case a serial number or alpha-numeric code contained within the barcode and/or RFID chip may be read and associated with the deposit and bundle references. The container is preferably made form a non-conductive material to facilitate the reading of RFID chips inside the container. This then marks the end of processing at the customer end of the process flow.

[0202] At step **1220**, the one or more containers containing the cash bundles are transported to the cash processing centre. This step is typically performed by a carrier operator who collects the one or more containers from the customer and delivers them to the cash processing centre. In the present example, the carrier operator is equipped to scan each container with an RFID reader. This allows the bundle identifiers associated with RFID chips attached to each bundle to be read inside the container. These identifiers can then be associated with the carrier and/or route details such as the present driver or security personnel, the time and date of collection, and other relevant information. The bundle identifiers may be associated with the carrier and/or route details in a database record and stored locally in a storage device present within the carrier vehicle. These records may then be downloaded upon arrival at the cash processing centre. Alternatively, each vehicle or carrier operator may be provided with a wireless or mobile data entry device, such as a PDA or mobile phone. This device may also comprise the RFID reader and a barcode reader and thus the header and container identifiers read from the container may be transmitted wirelessly to a central server wherein the deposit records can be updated accordingly. If these carrier details are linked with the header identifiers then they may be retrieved from the central database using the identifiers as an input to a query at step **1225** when the containers are scanned on arrival in the reception area **151**.

[0203] Once the one or more containers reach the cash processing centre, steps **1270** are performed within the centre. The present example will be described in relation to a cash processing centre such as that described in the second embodiment. However, it is also possible to use a cash processing centre as described with relation to the first embodiment. Hence, when the one or more containers containing the bundles of banknotes arrive at the cash processing centre, they enter into the reception area **151** wherein reception processing **150** begins. However, in contrast to the reception processing **150** of the second embodiment, the use of RFID chips associated with each cash bundle greatly simplifies the steps that need to be performed by the operator in the reception stage. Instead of entering deposit details into a user interface, the operator in the reception area **151** simply scans each container at step **1225** with a RFID reader to obtain the serial numbers of all the cash bundles present within the scanned container. Alternatively, this scanning may be performed automatically by a scanning gate at the entrance to the reception area **151**. These serial numbers are then processed by the reception module of the vault management system. This processing typically involves using the serial numbers in a database query to retrieve the deposit records generated at steps **1205** and **1255** within the retailer's premises. For example, the reception module may access a central server or

database wherein the deposit and processing information related to each bundle identifier is stored. Once the deposit reference associated with the one or more cash bundles is retrieved, data related to that deposit, such as the customer name and address, total value of the deposit or any other preadvised data that was entered at the customer's premises, may be displayed onscreen for visual verification by the operator in the reception area **151**. The reception processing **150** may also involve verifying that all the RFID serial numbers associated with bundles placed in each container by the customer are also detected on the scan performed by the operator. If one or more RFID serial numbers are not detected, or alternatively one or more RFID serial numbers not associated with the customer's deposit are detected, then this is recorded and a warning may be flagged to the operator or their supervisor. If the RFID serial numbers match, the one or more containers and/or the RFID and/or barcode serial numbers associated with each cash bundle within each container are assigned to the current operator and/or area. If a scanning gate is provided at the entrance to the reception area, the carrier vehicle or containers from the vehicle may be scanned on entry to the reception area **151** to check for the presence of RFID chips. If a scanning gate is used audio and/or visual and/or tactile feedback may be provided to indicate when a container has been successfully scanned. Scanning gates are particularly useful to track RFID items crossing boundary **140**, i.e. entering the vault. The serial numbers read back from located RFID chips may then be reconciled with the data recorded by the carrier operator.

[0204] In one particular embodiment, the RFID reader may be part of a thin, wall-mounted, dual-purpose scanner and display that would enable scanning on receipt. Such a scanner and display may comprise one or more of: a multi-directional barcode laser scanner, an RFID reader and antenna, a wireless networking module and/or fixed network capability, a large display and/or keypad for input. The scanner and the display are preferably constructed to withstand a collision from a trolley or other heavy apparatus within the cash processing centre.

[0205] As in the second embodiment, after the containers have been scanned in the reception area **151**, the cash bundles are transferred to the deposit processing area **111** wherein deposit processing **110** is performed. Typically, deposit processing **110** is performed in a similar manner to that described in the fourth embodiment, however, the various steps described herein may also be performed manually in association with the deposit processing described in relation to the first embodiment. The transfer of ownership to the deposit area and/or deposit operator may involve logging the transfer of the bundle identifiers to keep track of all bundles of cash.

[0206] At step **1235** the cash bundles are removed from the one or more containers and prepared for processing by a banknote sorter. In contrast to the fourth embodiment, the cash to be counted and processed is already provided in bundles with separator documents and therefore these cash bundles may be simply retrieved from the one or more containers and placed on a deposit tray ready for feeding to a currency sorting machine **260**. The currency sorting machine **260** is typically adapted to either read the barcode serial numbers present on one of the separator documents or the RFID serial number on each cash bundle at step **1240** and thus is able to look up the deposit identifiers related to the bundle identifiers and then record processing data generated by the currency sorting machine **260** against the deposit record. For example, as in the fourth embodiment, the currency sorting machine may incorporate one or more of counting authentication, fitness and denomination sorting. Information related to one or more of these areas may be stored under the deposit reference that is linked to the presently processed cash using the bundle identifier. This is shown in step **1245**.

[0207] This then allows the sort information associated with each bundle that was recorded at the customer's premises to be reconciled with the sort information generated by the currency sorting machine **260**. Any errors, irregularities or discrepancies may then be reported to senior personnel and recorded against the deposit. For example, the counted value of each bundle, as calculated by the currency sorting machine **260**, may be compared with the value of each bundle as entered or calculated during deposit processing at the customer's premises. In one example, if the serial numbers of each banknote in a given bundle were recorded during deposit processing at steps **1265** then these could be checked against the serial numbers of each banknote as recorded by the currency sorting machine **260**. After processing by the currency sorting machine **260**, the separator documents are removed from the bundles as the cash is typically resorted and recombined with other deposits for ease of deposit into the vault **121**. In this case, the separator documents are sent to a reject pocket such as **1014**R in FIG. **10**, which involves deallocating the serial numbers of the separator documents from the deposit at step **1250** so the same separator documents may be reused for other deposits. For example, the separator documents can be recollected and resent to the customer for future deposits.

[0208] Several variations of the fifth embodiment may be applied without deviating from the scope of the present invention. Instead of bundling the cash to be deposited, a durable plastic tag containing an RFID chip may be included in the deposit container together with the cash to be deposited. A serial number associated with the tag is associated with the deposit by either scanning the tag with an RFID reader, scanning a barcode printed on the tag or manually entering a serial number printed on the tag. Deposit information produced by the customer is then associated with the serial number of the tag. On arrival at the cash processing this tag may be read and processed in a similar manner to the separator documents described previously. The tag may be also scanned by the carrier operator during delivery.

[0209] If the security of the deposit is monitored from the time of customer deposit processing to deposit in the vault **121** then the methods of the fifth embodiment may be used to enable the value of the deposit to be added to the customer's financial account at the date and time of customer deposit processing, i.e. enable customers to pass value at source.

[0210] A further variation of the fifth embodiment uses RFID devices with a quantity of writeable memory. The customer is equipped with a RFID writer that enables the previously discussed deposit and/or processing data related to each banknote bundle and/or total cash deposit to be written to a memory within an RFID device associated with the bundle and/or deposit. Hence, instead of retrieving deposit and/or processing data using the serial numbers of the RFID chips, such data may be read directly from the memory of the chip itself.

[0211] A sixth embodiment of the present invention is illustrated in the flowchart of FIG. **13**. This embodiment uses radio frequency identified (RFID) devices in order to simplify

the order preparation process by allowing the bulk scanning of outgoing customer orders to verify their contents.

[0212] One set of processing which is performed during vault processing **120** is the re-bundling of sets of banknotes in bundles of a predetermined denomination and optionally of a particular fitness. Each bundle is then secured with one or more plastic straps. The strapping process may also be performed by a strapping machine that is adapted to sort and process the banknotes before automatically applying straps to any sorted bundles.

[0213] In the present case, RFID devices or tags are embedded or attached to the banknote straps that secure each bundle and this RFID tag is used to identify the bundle and optionally to store data related to the notes within the bundle. Each RFID device may resemble that shown and described in relation to FIG. **14**. The method of FIG. **13** shows a suitable strapping process. At step **1305**, a quantity of banknotes are sorted and processed. This may involve a manual sort or may involve a sort by a banknote sorter or strapping machine. Examples of sort criteria are denomination, currency, fitness, issue, or banknote recycling framework (BRF) type. The output of this sorting process is typically a bundle of banknotes with predetermined properties, for example 100×10 euro banknotes. At step **1310**, a strap is applied to the sorted bundle of banknotes to secure the bundle. This strapping process may be performed manually by an operator or may be performed by a strapping machine. At step **1315**, an RFID serial number or alpha-numeric code associated with an RFID tag attached or embedded within the current strap is read and recorded by the vault management system. This read operation may be performed by the strapper machine using an inbuilt reader or may be performed by the operator using a handheld reader. It is also possible to read the strap identifier before step **1310**. Once the serial number or alpha-numeric code of the RFID tag has been read, a data record is created, wherein the properties of the bundle of banknotes, as recorded by the strapper machine or the operator, are associated with the strap identifier. Hence the properties and value of the bundle of banknotes may be recalled using the strap identifier as an index. The properties of the bundle of banknotes may include one or more of: number of notes, denomination of notes, quality or fitness of notes, issue number, banknote serial number etc. This association of the bundle data with the strap is performed at step **1320**. In alternate embodiments, steps **1315** and **1320** may comprise writing the processing data related to a bundle of banknotes onto memory coupled to the RFID tag mounted in the strap. In this case, the strapping machine or the operator will be equipped with an RFID writing device which will write the required information to the memory coupled to the RFID tag.

[0214] At step **1325**, a decision is made as to whether strapped bundles of banknotes should be strapped into bundles of even larger value. For example, a number of bundles each containing one hundred banknotes of a particular denomination may be strapped to form a larger bundle of a thousand banknotes of that denomination, i.e. by strapping ten previously strapped bundles. Again, this may be carried out by a suitably adapted strapping machine or by an operator. If strapping of strapped bundles is required, then the strapped bundles are themselves strapped at step **1335** and a strap identifier or serial number associated with an RFID tag attached or embedded within the strap applied to the strapped bundles is read at step **1340**. The data associated with the previously strapped bundles and the further strapping process is then associated with the strap identifier of the larger bundle at step **1345**. For example, if ten previously strapped bundles are to be strapped to create a larger bundle, then the strap identifiers of the ten previously strapped bundles may be registered with the strap identifier of the strap wrapping the previously strapped bundles. After the bundles of banknotes have been strapped one or more times, the strapped bundles are either stored or moved to an area where they may be ready for order processing at step **1330**. Typically, the method **1300** is performed within the vault area **121** although it may alternatively be performed as part of the deposit processing **110** or the order processing **130**.

[0215] The bundles of banknotes are then used to pick an order as shown in FIG. **6**. An order is received from a customer and the ownership of the bundles is transferred from the vault area **121** or a vault operator to the order processing area **131** or an order processing operator. The order is then manually picked and a bag or container is filled according to this order. During this stage the order processing operator may optionally read the RFID serial numbers of the bundles and store these serial numbers with the customer order record. This may facilitate future auditing and customer management. After the order has been picked at step **640**, the container or bag can now be sealed as each bundle of banknotes within the bag or container has been strapped with a strap incorporating an RFID tag; to verify the value of a container or bag all the operator need now do is to scan the bag or container with an RFID reader which will retrieve the RFID strap identifiers and/or the value of notes from RFID memory. If the strap identifiers are read, then these can be used as an index to a central database to retrieve the value of the bundles. Hence the value or other details of a sealed order may be verified at any other further point after the order has been picked, including during despatch processing **160**. For example, before an order is loaded onto a carrier for transport to a customer, the sealed bag or container may be scanned by an operator using a handheld RFID scanner to confirm that the contents agree with the details of the order placed by that customer. As well as verifying the contents of an order using data retrieved from the RFID devices, further verification may be performed by weighing the container. Using order data retrieved from the vault management system the expected weight of the order may be calculated and compared with a measured weight of the order. This verification would involve adjusting for the weight of the container and straps. A more precise expected weight may also be calculated using the banknote data retrieved after reading the strap identifiers of the bundles within the container.

[0216] Additionally, the RFID tags on the bundle may be used to transfer ownership of the bundles. For example, once a bundle is strapped, it may be assigned to an operator in the vault processing area **121**. During transfer of the bundle from the vault processing area to the order processing area **131**, ownership of the bundles may be transferred as well using the methods of the present invention. This method may also allow the automatic picking of orders through automatically reading the RFID serial numbers of bundles to ascertain their value and then to use this information to automatically pick a predetermined quantity of notes for an order.

[0217] The final recipient of the cash order may also use the RFID devices attached to the strapped bundles to check that their order is correct. By scanning a container containing one or more tagged bundles that comprise a cash order, the recipient is able to confirm the value of a sealed container as

discussed above. This may be performed by receiving and integrating data stored in memory coupled to each RFID device or may be achieved by using the serial numbers associated with, and read from, each RFID device to perform a query on a central database to which the customer has access. In this manner the customer may check that their order is complete before opening the container and officially accepting a delivery of an order.

[0218] As well as associating details of the banknotes with the strap identifier at step **1320**, other details relating to the processing may also be associated with the serial number or alpha-numeric code of the RFID tag. For example, data such as the date of strapping or processing, time of strapping or processing, operator in charge of strapping or processing, sorting machine, strapping machine, processing performed, and/or area of processing may be associated with the RFID tag. Again, this association may be performed by storing data within memory coupled to the RFID tag or may be performed by associating the serial number or alpha-numeric code of the RFID tag with data in a database record stored within the vault management system. If a problem arises with a particular bundle of banknotes, useful data can be retrieved from the vault management system: for example, the exact machine that produced the strap may be investigated and/or the time of strapping may be linked to the security camera system in order to allow a visual check of the strapping process; alternatively if there is a note quality or authenticity concern, the sorting or strapping machine ID may be used to retrieve the sort parameters active at the time of sorting or strapping.

[0219] In the above embodiment an identifier comprising a serial number or alpha-numeric code is associated with a bundle of banknotes by way of an RFID device embedded in the strap of the bundle. In one variation the RFID device need not be used and the identifier is printed on each strap or bundling device by the cash processing system. In another variation strapped bundles may need to be separated before being deposited in a container. If this is required the RFID devices in each strap may be scanned before the strap is removed and the banknotes in the bundle are placed in the container. At this point data comprising properties of the banknotes in each bundle may be retrieved using the scanned identifier. Such data may then be associated with an identifier of the container. This technique may be used, for example, when filling an ATM cassette.

[0220] While the method of the sixth embodiment has been described in relation to a strap it is also possible to use alternative means to secure sorted numbers of banknotes. For example, output cassettes, plastic containers or envelopes may alternatively be used, wherein an RFID is inserted or attached to the cassettes or envelopes. In these cases the strapping machine will be adapted to output the collection of banknotes in the required form. The RFID tag may also be incorporated into a print-on-demand label which may then be attached to a bundle of notes.

[0221] To facilitate the transfer process described in relation to FIGS. **3**A and **3**B radio frequency identification devices or RFID tags may be installed upon the containers used to transfer the cash. These RFID tags may be used in a similar way to the barcodes present on the containers that were described earlier.

[0222] An example of a suitable RFID tag is shown in FIG. **14**. The tag **1400** comprises a tag substrate **1410**, an aerial **1420**, a controller **1430** and optional memory **1450**. The controller may comprise an integrated transmitter and/or receiver. Tag **1400** is passive and so has no internal power source. The aerial **1420** receives power from an external reader. Radio frequency signals emitted from the external reader impinge on aerial **1420** and enable the controller **1430** to modulate the received signal or to "backscatter" a carrier wave to return a signal to the external reader carrying information related to the RFID tag **1400**. Typically the tag **1400** comprises memory **1450** which contains a serial number or alpha-numeric code. This serial number or alpha-numeric code identifies the tag and typically comprises a plurality of bits of data. Upon receiving a radio frequency signal from an external reader the controller **1430** is typically adapted to modulate the received signal in such a way that the tag identifier can be extracted from signals received back at the external reader.

[0223] A tag **1400** as shown in FIG. **14** may be applied to a container to facilitate the transport process shown in FIG. **3**A. In the previously described example, at step **325**, a barcode applied to the container was scanned in order to achieve a serial number or identifier related to the container. In the present case at step **325** an RFID tag applied to a container may be scanned to retrieve a serial number or other identifier associated with the tag. If this serial number was previously associated with the deposit items within the container then details relating to the deposit items within the container may be retrieved from central database **215** by scanning the tag and retrieving the serial number. By using an RFID tag instead of a barcode, information may be gained concerning the deposit items within a container from a distance. This may enable multiple containers comprising RFID tags to be scanned in a set area before a plurality of containers are transferred. To reduce interference and transmission problems the containers may be constructed from a material that does not interfere with the propagation of E-M radiation, for example certain polymers.

[0224] A container equipped with an RFID tag may also be used to record the events surrounding a transfer as described in FIGS. **3**A and **3**B. For example if a cash processing centre resembling FIG. **1**D is used a number of passive gates adapted to interrogate RFID tags may be installed at gateways **156**, **116**,**126** and **136**. When a container comprising an RFID tag is passed through one of these passive gates, i.e. through one of the gateways **156**,**116**,**126** or **136**, the RFID tag is detected and its serial number retrieved by control systems attached to the passive gates. This then allows a transfer event to be generated documenting that a transfer has occurred between two neighbouring areas joined by the detecting gateway. To determine the direction of travel of the container the retrieved serial number of a detected RFID tag may be used to query central database **215** to retrieve the last location record concerning the RFID tag in question. This retrieved location then becomes the source location and the other area bordering the gateway becomes the destination region. For example, if a container was last registered as being within deposit processing area **111** and is detected passing through gateway **116** then it is assumed that a container comprising a detected RFID chip is moving from deposit processing area **111** to vault processing area **121**.

[0225] In order to provide a closed system, passive gates may also be provided on all entrances and exits to the cash processing centre. For example, turning to the exemplary cash processing centre shown in FIG. **1**E passive gates may be mounted around the entrance to reception area **151** and dispatch area **161**. When a plurality of containers enter the recep-

tion area **151** within a delivery vehicle then the RFID tags associated with those containers may be detected and the serial numbers associated with the detected tags may be entered in to location records in central database **215**. A location record will thus record the detected containers as being located within reception area **151**. Likewise when a number of containers in a delivery vehicle that contain customer orders leaves dispatch area **161**, a passive gate will detect the RFID tags within the vehicle and record the associated containers as having left the cash processing centre.

[0226] If methods and apparatus according to the fifth or sixth embodiments are used then individual cash bundles may be tracked on entry and/or exit to particular areas using RFID tags located in either the header or trailer documents or the straps of bundled banknotes.

[0227] To facilitate end-to-end tracking of deposits throughout the deposit process each deposit may be linked to a particular deposit identifier from pre-advertisement at the customer's premises to deposit processing and reject handling. To do this a particular RFID identifier related to a particular RFID tag may be associated with a container containing the deposit. The container and/or the RFID tag then stays with the deposit throughout the deposit lifecycle. RFID readers at predetermined locations may then detect the RFID tag and retrieve the identifier. This then allows real-time deposit tracking. For example, RFID readers may be provided within CIT vehicles, in the reception area **151**, at the preparation and machine entry areas within deposit processing area **110**, near or on cages temporarily storing deposit containers or within the vault. A similar system may also be used to track customer orders from the vault to the dispatch area and even possibly the CIT delivery vehicle. This would then allow complete tracking from and to the customer.

[0228] The tracking of items within the cash centre using RFID technology may be passive, based on the location of the last recorded transaction involving the RFID tag, or active, using the properties of the RFID tag to track the location of the tag in relation to one or more RFID readers positioned nearby. For example, a container having an RFID tag and being positioned on a cage in a first area awaiting transfer to a second area may be located by an overhead RF antenna positioned in the first area. The tracking system may also be used by CIT operators to retrieve real-time information on the status of cash orders. A plurality of RFID readers at a variety of stages during order preparation and dispatch may replace or complement existing CIT tracking systems. Using a single tracking method incorporating RFID would, however, greatly simplify the process.

[0229] An example of a deposit sequence using the methods discussed above is shown in FIG. **19**. At step **1910**, an RFID tag attached to a container is detected on entry to the cash processing centre (CPC) and an entry event is generated at step **1940** and stored in central database **215**. The RFID identifier associated with the RFID tag is also retrieved and stored in the entry event record. The vault management server **210** is then configured to, at step **1915**, use the retrieved RFID identifier to retrieve a pre-advisement record containing deposit data that was generated by the customer and sent to, or recorded in, central database **215**. At this point the vault management server generates an ownership transfer event at step **1945** to assign ownership of the deposit stored within the tagged container to the reception area **151**. The deposit may be referenced using the deposit reference generated in step **1255** of FIG. **12**. After reception processing has been performed the container, and thus deposit, is moved at step **1920** to the deposit processing area **111**. This typically involves passing the container through a gateway with an associated RF scanning reader attached. The scanning reader detects the RFID tag attached to the container and sends a message to the vault management server **210**. The vault management server **210** then looks up the previous position of the RFID tag (or associated deposit) and uses this to determine the direction of travel through the gateway. The vault management server **210** is then configured, at step **1950**, to generate a transfer record indexed by the retrieved RFID identifier of the RFID tag and to assign ownership of the associated deposit to the deposit processing area **111**. At step **1925**, an operator or banknote sorter scans the RFID tag before deposit processing takes place so that data generated by the deposit processing can be compared, and possibly reconciled, with the original deposit data generated as part of steps **1265** in FIG. **12**. This comparison is performed at step **1955** and the result is stored in the central database **215**. After deposit processing, at step **1930**, the container is repacked with the deposit and then transferred to the vault processing area **121** for unloading and storage. During the physical transfer of the container from the deposit processing area **111** to the vault processing area **121**, another gateway scanning reading detects the RFID tag and a transfer record and ownership assignment are generated at step **1960**, in a similar manner to step **1950**. Within the vault the container is unpacked and the RFID tag attached to the container is de-allocated from the deposit removed from the container at step **1935**.

[0230] Some advantages of the RFID technology described above are:

- **[0231]** efficient confirmation of containers and/or bags received from a CIT vehicle, by using RFID tags to track deposits and provide associated data manual counting and/or quantity reconciliation is avoided;
- **[0232]** efficient loading of deposit and manifest data for further sorting during deposit processing, this increases the speed with which transfers between areas can be achieved;
- **[0233]** the presence of deposits to be processed and their corresponding location can be ascertained;
- **[0234]** manual typing and its associated risk of error is reduced;
- **[0235]** the presence of articles of value in the vault area may be accurately ascertained, together with the entry and exit times of such items; and
- **[0236]** all items that are ready to be placed in the vault can be monitored.

[0237] RFID technology may also be used to facilitate the processing of secure cassettes for automated teller machines (ATMs). Such cassettes are typically mounted within ATMs and supply cash for withdrawal. U.S. Pat. No. 6,976,634 B2 provides an example of a secure cassette and its use within an ATM, wherein the cassette may be supplied with an embedded RFID tag. A cassette may also be compartmentalised to store different types of currency; for example, a cassette may have one compartment to supply cash to the ATM for withdrawal by a customer, one compartment to store any notes that have been rejected by the ATM, and a third compartment for cash deposits made into the ATM.

[0238] The presence of an RFID within the structure of the cassette or deposited with cash within the cassette may facilitate the reconciliation process performed when the cassette is returned to a cash processing centre. The lifecycle of a cas-

sette begins when it is selected as a container in order processing **130**. The cassette may be filled according to the steps shown in FIG. **6**. At step **635** an RFID alpha-numeric identifier associated with the cassette may be registered with the order being processed. This may be performed by scanning the cassette with a hand-held RFID reader. After the order has been picked at step **640**, data associated with the order, such as total cash amount, denominations present and note quality may optionally be wirelessly loaded onto memory coupled to the RFID through the RF channel. Such memory may form part of the RFID itself or the electronics of the cassette. During despatch, delivery and installation the RFID may be used to track the physical location of the cassette as described above. After installation the ATM may access the memory coupled to the RFID, either through the RF channel or a local connection to electronics within the cassette, and download data associated with the order to update its own records.

[0239] During use and/or before removal of the cassette, the ATM may communicate with the memory to update various fields of data. For example, the ATM may record details of all cash withdrawn from or deposited into the cassette and details of notes deposited into a reject compartment. Depending on the size of the memory and the hardware of the ATM, this data may relate to individual notes indexed by serial number or may relate to final totals for each compartment. The ATM and/or cassette may also be adapted to determine when data values indicate that the cassette requires emptying or refilling and automatically place an order for pick-up and delivery to the cash processing centre.

[0240] After removal and delivery to the cash processing centre, data stored with memory may be read by operators in the reception **150** and/or deposit processing **110** stages. For example, in a similar manner to the "pre-advisement" methods described above, the operator may scan the RFID, download data concerning the cash contained within the cassette and use such data to populate fields within the vault management system **200** in preparation for the reconciliation performed during deposit processing **110**, e.g. automatically obtain the data required to perform steps **515** as shown in FIG. **5**A.

[0241] In certain circumstances, ATM reliability can be increased if secure cassettes are matched with individual ATMs. For example, mating mechanisms on both cassette and ATM may wear and be displaced over time; however, for a given cassette and ATM pairing such wear and displacement will be complementary. To facilitate the correcting pairing of a given cassette and ATM, an RFID may be used.

[0242] According to a particular embodiment, the secure cassette is permanently associated with a particular RFID. For example, the cassette may be fitted with a read/write (R/W) RFID coupled to a memory. The memory may comprise a protected area that is read-only; this area contains a data identifier. The data identifier may be permanently associated with an ATM identifier, either via intermediary means, such as an association in a relational database, or directly, i.e. the data identifier may comprise the ATM identifier. When a paired cassette is required, the order, as described in the method of FIG. **6**, stipulates that a cassette with a particular data identifier must be used. The operator performing the order processing **130** then locates a or the cassette with the stipulated data identifier and scans the cassette with an RFID-reader. If the cassette does not have the required data identifier the order processing module will not allow the operator to continue with the order processing **130**. If the cassette does have the required data identifier the operator fills the cassette as discussed in relation to step **640** and may additionally upload data related to the order to the memory. The cassette may then be dispatched, delivered and installed in the appropriate paired ATM dictated in the order. The ATM may also be able to download the order data from the memory as described above.

[0243] Another use of RFID tag **1400** is shown in FIGS. **15**A and **15**B. In this example the cages or trolleys that are used to respectively store or transport containers within the cash processing centre are equipped with RFID passive scanning gates in order to detect any RFID tags placed within them. If each RFID tag is associated with a container then the location of containers containing cash deposits can be traced throughout the cash processing centre. FIG. **15**A shows an end view of a trolley **1510** for transporting containers around the cash processing centre. The trolley **1510** has a number of wheels **1520** which enable it to be wheeled around the different areas of the cash processing centre. The trolley **1510** is further provided with one or more RFID passive scanning readers **1530** which are attached to the trolley **1510**. In the present example the trolley comprises four passive RFID readers, one mounted in each vertical corner member of the trolley. In use, the trolleys transport a number of containers **1550** around the cash processing centre. These containers **1550** have an associated RFID tag **1400**, for example wherein tag substrate **1410** is affixed to the side of a container. At predetermined intervals each passive scanning gate **1530** will emit a number of radio frequency signals **1314** which are used to detect the presence of an RFID tag within the range of each passive scanning reader. An RFID tag may be detected by modulating or backscattering the radio frequency signals **1540** as described earlier. Thus the serial number or identifier associated with any RFID tag in the location of each passive scanning reader may be retrieved. In FIG. **15**A no container is placed upon the trolley **1510** and thus no backscatter signal is received by the passive RFID scanning readers **1530**.

[0244] FIG. **15**B shows a side view of the trolley **1510**, wherein a container **1550** has now been placed upon the trolley. When a container **1550** comprising an RFID tag **1400** is placed upon the trolley **1510**, the RFID tag **1400** backscatters one or more of the radio frequency read signal **1540** emitted by the passive scanning readers **1530**. In the example shown in FIG. **15**B, passive scanning reader **1530**A is the closest device to container **1550** and so reader **1530**A receives a response signal **1560** that has been modified by tag **1400**. Reader **1530**A thus detects the response signal **1560** and decodes the serial number associated with RFID tag **1400**. Hence, the number of containers present within the trolley **1510** may be detected by the passive scanning readers **1530** and the serial numbers of each tag attached to each container may also be retrieved. In the present example the trolley **1510** is mobile and so the trolley further comprises a wireless transmitter **1570** which allows the reading apparatus **1530** to communicate over a wireless network with the vault management system running on server **210**. The serial numbers associated with the RFID tag can then be related to containers and deposits so that the location of each deposit may be known.

[0245] A cage may also be adapted as described above and will typically resemble the trolley **1510** in FIGS. **15**A, **15**B without the presence of the wheels **1520**. Both cages and trolleys may be provided with doors and/or panels on one or more sides of the frame **1510**. The passive scanning readers **1530** may alternatively comprise a closed loop antenna

mounted around the edges of the cage or trolley, e.g. forming a closed loop around all four edges of the trolley or cage. The passive scanning readers **1530** may also be placed on the top and bottom of the cage and/or trolley as well as or instead of being placed on the sides of the trolley and/or cage. As a cage is typically stationary the detection control systems linked to the passive scanning readers **1530** may also be linked to the central databases over a standard wired Ethernet link. The RFID tags may also comprise active or powered RFID tags and thus the passive scanning readers **1530** will comprise active scanning readers.

[0246] By using cages and/or trolleys with built-in RFID scanning readers the vault management software is able to track which containers move in and out of each trolley and/or cage within the cash processing centre. Hence, an operator or manager may be able to instantly find out the value of any cage and/or trolley within the centre by retrieving the cash or deposit information that has been associated with each container or the RFID tag **1400**. In certain cash processing centres each cage and/or trolley may have a certain insurance limit. This means that the cage and/or trolley can only be loaded with a certain amount of cash. The RFID scanning reader thus allows the value of any cage and/or trolley to be calculated by the vault management system and if the insurance limit is exceeded then a warning can be displayed. Events that record when a container **1550** enters a cage and/or trolley may also be used together with CCTV systems to retrieve video footage of the container being placed into the cage and/or trolley or being removed from the cage and/or trolley.

[0247] In a variation to the apparatus shown in FIGS. **15**A and **15**B the trolley **1510** may itself comprise an RFID tag **1400**. When a container **1550** is placed upon the trolley **1510** the RFID tag of the trolley and the RFID tag of the container are read by a handheld reader or a static reader in the vicinity of the trolley. The identifier of the RFID tag attached to the trolley is then linked to the identifier of the RFID tag attached to the container on the trolley. The trolley and the container may then be linked within the vault management system, e.g. within database **215**, to allow the location of container **1550** to be ascertained. At certain intervals a RFID scanning reader external to the trolley **1510** may then be used to scan the trolley to verify that the records stored within the vault management system, i.e. the number of container tags present on the trolley, match the data stored in the database.

[0248] In a similar manner, the trays that are loaded with cash deposits before processing by a banknote sorter or currency sorting machine may also comprise an associated RFID tag. If the methods of identifying bundles of cash used in the fifth and sixth embodiments are used then the bundles of cash present upon a tray may be linked with an identifier associated with the RFID tag attached to the tray by scanning the tray any accompanying deposits with an RFID reader. This then returns the tray tag identifier and the deposit identifiers which can then be linked within the vault management system. Hence the vault management system is able to keep a record of the expected value of each tray within the cash processing centre. By keeping track of the value of each bundle of cash placed on the tray a manager may also be provided with information about the total value of cash upon the tray. This total value of the tray may be used to keep within insurance limits and/or used to track whether there is enough deposited cash to keep the banknote sorter or currency sorting machine running at a predetermined capacity. If a tray is scanned before a processing operation upon the currency processing machine **260** is performed, then the data associated with the processing of the deposits upon the tray may be verified against data related to the deposits that were recorded before the operation. The banknote sorter or currency sorting machine may also be adapted to use a list of expected cash bundle or header card identifiers and thus the sorter or machine may be further adapted to stop operation if an RFID tag is detected that has an identifier that is not on the list. This technique may also be used to pair users and devices or storage containers and units.

[0249] An extension of the use of RFID tags and RFID readers to ascertain the location of cash within the cash processing sensor, both in the form of customer deposits and orders, involves the use of an advanced active RFID device in association with a wireless positioning system. The example below is described in relation to a wireless trilateration system, however the methods and systems may be adapted to operate using other known positioning systems, such as those that involve wireless triangulation or global positioning systems such as NAVSTAR GPS.

[0250] Wireless trilateration systems typically allow location tracking of suitably adapted RFID devices using a wireless local area network (LAN). Typically, an IEEE 802.11 compliant wireless LAN is constructed with a plurality of wireless access points. A RFID device is then adapted to communicate with these access points upon the wireless LAN using standard protocols and each RFID device may be uniquely identified by an address string such as the network MAC address of the RFID device. In use, when an RFID device communicates with three or more wireless access points the RFID device may be located by examining the signal strength of radio frequency communications between the RFID device and each of the three or more access points. Such a system is easy to implement using existing wireless LAN infrastructure that has been designed for data communication. An example of a suitable wireless trilateration system is that provided by Pango Networks Incorporated.

[0251] A seventh embodiment of the present invention directed to a wireless trilateration system adapted for use in a cash processing centre is shown in FIG. **17**. This example features a simplified cash processing centre as described in relation to the first embodiment; however the wireless trilateration system may be expanded for use in a cash processing centre of any size or layout. Each area of the exemplary cash processing centre **106** has a number of wireless access points **1720**. In the present example, two wireless access points are positioned in the deposit **121** and order **131** processing areas and four wireless access points are positioned within the vault processing area **121**. The access points are positioned so that an RFID device located anywhere within the cash processing centre will be able to communicate with at least three access points at any one time. In the present example, the access points are connected to a wired Ethernet network **1730**. This wired network **1730** is connected to a location server **1710**. The location server **1710** is configured to send data to and receive data from the access points **1720**.

[0252] Location server **1710** is connected to the vault management server **210** via a network comprising router **235**A. Hence, the location server **1710** is integrated into the vault management system in a similar way to the CCTV system shown in FIG. **8**. The location server **1710** is also accessible from a remote client workstation **220**C. This remote workstation **220**C communicates with the server **1710** via router

235B, WAN 245 and router 235A. In certain embodiments of the present invention the location server 1710 may be incorporated within the vault management server 210 rather than being incorporated in separate hardware as shown in FIG. 17.

[0253] Articles to be tracked within the cash processing centre are typically equipped with an RFID device. These articles may comprise one or more of cages, guns, employees, bullion, trays, containers, cash bundles, trolleys, banknote sorters, and any other equipment used within the cash processing centre. Each RFID device is designed to communicate with the access points 1720 forming the wireless LAN. In use, due to the careful positioning of the access points within the cash processing centre, each RFID device should be able to communicate with at least three access points.

[0254] In the present example, the RFID device is adapted to emit a radio frequency signal or "chirp" containing a unique device identifier at predetermined intervals. For example, the RFID device may emit a number of bits comprising the device MAC address at 20-second intervals. This signal or chirp is detected by any access points within range of the RFID device. Each of the access points within range then processes the received signal or chirp and forwards a message comprising the detected signal strength of the received signal and the unique device identifier to the location server 1710 over network 1730. The location server 1710 is then adapted to use the received signal strength and device identifier from at least three access points to calculate the position of the RFID device and hence calculate the location of the article of interest. Typically, this is achieved by calculating the distance of the tagged object from the at least three receivers based on the signal strength and known signal attenuations over a set distance. The position of the object can then be found using standard geometry. Using such a system articles can typically be located to within 0.5 meters.

[0255] In an alternative embodiment, directional antennas may be used in a triangulation system to detect the position of a tagged object. In this case only two directional receivers need be used. When a "chirp" is received from a tagged device each receiver records the direction in which the "chirp" has a maximum measured power or intensity. Two angles are then calculated from the directions detected by both detectors and these angles are used together with the known distance between the detectors to calculate the position of the object. Such a system could operate on similar hardware to that shown in FIG. 17.

[0256] In the present example, the calculated location is used to update a location database 1715. Location database 1715 may comprise an object orientated database comprising a collection of object records corresponding to each of the tagged articles within the cash processing centre. Each object record may be indexed and retrieved using the unique device identifier of the RFID device attached to each article. Each object record also has a location property. This location property may be given as a 2-dimensional coordinate corresponding to a location within the cash processing centre. To enable real time or near real time monitoring of articles within the cash processing centre this location property may be updated at predetermined intervals using the calculated location information.

[0257] FIG. 18 illustrates how the location server 1710 and location database 1750 are used to track articles within a cash processing centre. FIG. 18 shows an example client terminal or workstation 1840. This workstation could be remote workstation 220C as shown in FIG. 17. The workstation 1840 runs a location module that operates as part of the vault management system. This location module comprises a client application that operates upon the workstation 1840 and that communicates with the location server 1710 to provide location information. In alternative embodiments the client application may instead communicate with the vault management server 210, wherein the vault management server 210 in turn communicates with the location server 1710. The client application may be an Internet or "web" browser adapted to communicate with one or more of the location server or the vault management server acting as an Internet or "web" server.

[0258] The location module displays a schematic plan 1810 of the cash processing centre on a suitably designed graphical user interface. The location of various articles 1820 and 1830 are then superimposed on this plan 1810. This may be achieved by retrieving the location property of a given article from the location database 1715. In FIG. 18 a first article 1820 is shown as being located in the deposit processing area 131 and a second article 1830 is shown as being located in order processing area 121. The icons associated with each article may then move around the schematic plan 1810 in real-time as the location property of each object is updated by the location server 1710 (or near real-time depending on the update interval). The location module may further be adapted to alert an operator when a selected article travels to an unauthorized area, for example outside of the building limits. The location system shown in FIGS. 17 and 18 may also by integrated with cash in transit (CIT) tracking and GPS (Geographical Positioning System) data to provide the real or near real time geographic location of a deposit or a cash bundle.

[0259] In certain embodiments of the present invention, delivery and article routes may be displayed on a third party mapping system that provides schematics maps of the area or country of operation, for example "Google Maps" provided by Google Incorporated of California, USA. Such routes may be generated with or without the tracking system described above. Without the tracking system routes may be generated by passing parameters such as the post or ZIP codes of start and end destinations to a third party application programming interface. This parameters and any date and/or time data may be retrieved automatically from records stored in database 215. For example, a route may be generated using records pertaining to two or more of: a customer requiring a deposit, a CIT depot, the cash processing centre, a delivery address in a cash order etc. Each route may have one or more intermediate points. With the tracking system described above data may be passed to the mapping interface in real-time or at predetermined intervals. New routes may thus be created using this data or the data may be used to update and/or amend pre-existing routes. For example, a first route may be displayed from a customer address to the cash processing centre. Real-time location data may then be used to display the progress of a CIT vehicle travelling between the two locations, including timings and any detours taken. Such a map may be displayed to a customer making a deposit or awaiting a cash order, for example a customer operating a client device similar to device 220C. The mapping system may also provide a map of the customer's premises, the cash processing centre, and any stop off points along the route of the CIT operator.

[0260] The history of when a particular RFID tag was scanned and detected may also be added to the location map using transfer or detection event information stored in central database 215. By processing location data collected over

time, average timings of transport and standard routes both inside and outside the cash processing centre may be established. Security alarms may then be raised if an article is detected as deviating from an established route.

[0261] An RFID badge for use in tracking employees or operators using the methods described above is shown in FIG. **16**. The badge **1610** comprises a photo of the employee **1618** and a clip **1670** for attaching the badge **1610** to the employee's clothing. Inside the badge (as represented by dotted lines **1690**) is located an antenna **1620**, a controller **1630**, a power supply **1660**, and memory **1650**. The antenna **1620**, controller **1630** and memory **1650** operate in a similar manner to the passive RFID tag shown in FIG. **14**, however in the present case power supply **1660** allows a stronger signal to be emitted by antenna **1620** and more advanced processing to be performed by controller **1630**. Even though the badge in FIG. **16** is described as using active RFID methods, it is also possible to use the apparatus of FIG. **14** to produce a passive RFID badge. Each RFID controller **1630** may then be adapted to communicate with at least three access points **1720** within the cash processing centre to locate the employee.

[0262] As well as tracking employees around the cash processing centre the RFID badges may also be used to recognize the presence of an employee in front of a device and/or determine whether the employee is authorised to use the device. This may be performed in one of two ways.

[0263] In the first method, the triangulation system of FIG. **17** or any other suitable location system is used to track the employee. When an employee enters a location range in front of a particular workstation the vault management system may be adapted to compare the identity of the employee, their present location and their security status to automatically log them on to the vault management module relevant to their job with the cash processing centre.

[0264] In the second method, an RFID reader is used to detect the RFID badge **1610**. In this case, the RFID badge **1610** may comprise a RFID chip that may be read either passively or actively over a limited range. FIG. **20**A shows a schematic illustration of three devices: banknote counter or sorter **230**A, client workstation **220**A and handheld barcode or RFID scanner **225**. Each device has an associated RFID reader **2010**. The RFID reader **2010** may be provided independently of the device, for example attached on, to or under each device as shown in FIG. **20**A, or may be built into each device, depending on the circumstances. The devices of FIG. **20**A are provided as an example and other devices may be adapted in a similar manner, for example the large sorter shown in FIG. **10**. Furthermore, one or more RFID readers **2010** may be shared by one or more devices, for example the RFID reader **2010** may be located under a table worktop that is used by an operator operating all three devices in FIG. **20**A.

[0265] In FIG. **20**A, when an operator or employee wearing RFID badge enters within range of one or more of the RFID readers **2010**, the readers communicate with the RFID chip **1690**. Controller **1630** may then retrieve an alpha-numeric identification string, the "identifier", from memory **1650**, together with any other optional data, and transmit this back to each RFID reader **2010** using antenna **1620**. If the badge uses active RFID technology power will be supplied from power supply **1660**. Each RFID reader **2010** then receives the identifier and optional data and communicates with vault management server **210** and database **215**, typically over a wired or wireless network. The identifier and optional data may then be used to authenticate and/or authorise the operator or employee as shown in FIG. **20**B.

[0266] FIG. **20**B shows a method **2020** of authenticating and authorising a user. In certain embodiments only the authentication or authorisation steps may be performed. The method begins at step **2025** wherein a user equipped with an RFID badge **1660** enters into the proximity field, i.e. the range, of an RFID reader **2010**. Depending on the technology used, this activates a number of processes in RFID chip **1690** under control of controller **1630**. Controller **1630** then at least retrieves an identifier from memory **1650** and transmits this data at step **2030** to the RFID reader **2010** using antenna **1620**.

[0267] In the present example it will be assumed that RFID reader **2010** has limited processing capability and passes any received data to the vault management server **210** over network **231**. Vault management server **210** then performs the following processing steps. However, in other embodiments the following processing steps may be distributed across one or more devices including the RFID reader and/or a local workstation.

[0268] At step **2030** the received identifier is used to lookup user data. Such user data may be stored in a user account as described earlier. The identifier may be a primary key for the user account or may be associated with the user data in a relational database such as **215**. Alternatively, the identifier may identify a user group as described earlier. At step **2040** the user is authenticated, i.e. the user wearing the RFID badge **1610** is identified. If the use of RFID badges is strictly controlled then it may be assumed that the identified user is correct. However, in most cases this level of trust will not exist and a further password may be required to fully authenticate the user. For example, when the user comes into close proximity to RFID reader **2010**A, the banknote sorter **230**A may display an identified user name received from vault management server **210** and prompt the user to enter his or her password to confirm authentication. The password may then be entered using an input device of the banknote sorter **230**A. Even when a password is required this process reduces keying by a user by fifty percent. A similar procedure may be performed for client workstation **220**A. For devices such as barcode or RFID scanner **225** that do not have a display or input device, a further local device may be used to confirm the authentication. For example, a user may be shown his or her user name on nearby client workstation **220**A and be asked to enter his or her password using the keyboard of the workstation.

[0269] If the user is not successfully authenticated, for example if the identifier was not located in database **215**, a password was incorrect, or the user is no longer an employee, then access to the vault management system is denied at step **2045**. If the user is denied access an alert may be also triggered to inform security and management personnel of an unauthenticated access attempt has been made, together with the location and time of the attempt. At step **2035** video footage of the user, either a still or moving image, may be optionally captured to visually confirm identity or further biometric scans may be required instead of or as well as a password.

[0270] If the user is successfully authenticated a check is then made at step **2050** to determine if the user is authorised to use the device. Typically, this involves looking up user or user group data in a database such as database **215** for the authenticated user. For example, a binary flag stored within user or user group data may indicate whether the authenti-

cated user is authorised to operate banknote sorter **230**A. If the user is not authorised they are denied access to the device at step **2055**. An alert may also be logged. If the user is authorised they are allowed to access the device at step **2060**.

[0271] In certain embodiments, a single RFID reader may be provided for several devices. For example, in FIG. **20**A only RFID reader **2010**B may be provided. In this case, client workstation **220**A is used to authenticate the user. After authentication authorisation data may be retrieved from a database and used to lock any devices connected to client workstation **220**A for which the user is not authorised; for example, banknote sorter **230**A and/or barcode or RFID reader **225**.

[0272] The system and method of FIGS. **20**A and **20**B may be used as an additional security feature within the cash processing centre. For example, as well as preventing non-personnel from accessing vault management systems, in a particular embodiment the system and method may be used to only allow access to employees during their working hours, denying access outside of their official shift times. The system and method may also be used to comply with health and safety provisions. For example, a user may only be authorised to use a particular device such as large counter **260** in FIG. **10** once they have received proper training.

[0273] The system and method may also be used to control the configuration of devices. For example, the authorisation data retrieved for an authenticated user may be used to select and/or lock an appropriate banknote processing program; an operator performing a note count operation would not require denomination and/or authentication detectors on a banknote sorter, hence these detectors may be automatically switched off based on authorisation data for the operator. Alternatively, the authorisation data may be used to implement the dual control and module locking methods described above. For example, when a supervisor enters the proximity field associated with an operator's client workstation, the workstation screen may automatically prompt the supervisor for their password and activate the dual control configuration. Likewise, a deposit processing operator may only be authorised to access a deposit processing module and be denied access to an order processing module. Such configuration could further be based on a number of conditions, for example an afternoon shift may be limited to use a particular sorting process, which may differ from the process used by the morning shift. The user, and by extension the shift, may be identified and authorised using the method of FIG. **20**B, eliminating the need to manually reset devices between shifts. In this case, the vault management server **210** may apply configuration rules based on data available to it and received in step **2035**.

[0274] The authorisation may also apply to physical access. In certain embodiments an RFID reader may be applied to a cage or trolley, as shown in FIGS. **15**A and **15**B. However, instead of detecting the presence of a container as shown in these Figures, readers **1530** may be used to authenticate an operator and authorise access to the cage and/or trolley. If access is allowed the cage or trolley may be unlocked automatically, optionally for a predetermined time period. The cage or trolley may also be locked again once an identified user leaves the proximity field of an associated RFID reader. Similar methods may also apply to physical areas of a large banknote counter or sorter, for example a local RFID reader may authenticate a nearby operator and vault processing server **210** may determine if they are authorised to access internal sections or compartments of the counter or sorter and, if necessary, unlock such sections or compartments.

[0275] Even though the above system and method was described in relation to an RFID badge **1610**, it need not be limited to such a form. In an alternate or complimentary embodiment, the RFID chip may be embedded in a watch, wrist strap or bracelet worn by the operator or employee. In this case, a narrow field RFID reader may be placed underneath an input panel of the device, such as under a keyboard of client workstation **220**A. Hence, when the operator interacts with the input panel, the watch, wrist strap or bracelet will come into close proximity to the RFID reader and the RFID chip may be read without requiring any further action or input from the operator. This makes the technology more acceptable to employees as they do not have to alter their established routines to enable RFID authentication and authorisation. Alternatively, the RFID badge **1610** may be swiped or passed underneath an RFID reader in the usual manner to log in and out of the vault management system on a client workstation. RFID cards may also be used with biometrics and fingerprint identity systems. By combining the RFID badge with one or more additional security systems a manager can be confident that only authorized users may access the vault management system and thus be confident of the integrity of any information being inputted into the system. Data associated with the location of the employees may also be used to track employees working hours.

[0276] The above systems and methods have been described with relation to radio frequency identification devices; however, such systems and methods may also be adapted to operate with other related wireless transmission systems using optical, infra-red or microwave wavebands, acoustic technology such as ultrasound, mobile radio systems, cellular technology, and Bluetooth, ZigBee or Ultra-wideband (UWB) standards, amongst others.

[0277] Any of the methods described in this specification may be implemented in software using known software development techniques, in dedicated hardware using appropriately configured logic units or in programmable hardware adapted to process digital instruction sets.

1. A method of providing information about a plurality of entities within a cash processing centre, the method comprising:

coupling a first entity with a first wireless device;

coupling a second entity with a second wireless device;

reading data associated with both the first and second wireless devices; pairing data associated with both the first and second wireless devices; and

retrieving information concerning the relationship between the first entity and the second entity based on the pairing.

2. The method of claim **1**, wherein:

the first entity comprises a container for storing articles of value; and

the second entity comprises storage means for one or more containers;

the method further comprising:

storing data comprising the properties of one or more articles of value;

associating said data with the first entity;

storing the first entity on or within the second entity; and

retrieving information comprising the cumulative properties of the articles stored on or within the second entity based on the pairing.

3. The method of claim 1, wherein:
the first entity comprises one or more articles of value; and
the second entity comprises a unit adapted to store articles of value;
the step of retrieving information comprising:
retrieving information indicating that the first entity is stored upon the second entity.

4. The method of claim 1, wherein:
the first wireless device comprises a wireless transmitter configured to transmit a first identifier;
the second wireless device comprises a wireless receiver having a second identifier; and the step of reading data comprises:
transmitting the first identifier from the wireless transmitter;
receiving the first identifier using the wireless receiver; and
reading both the received first identifier and the second identifier of the receiving device.

5. The method of claim 4, wherein the method further comprises:
determining signal characteristics associated with the received identifier;
using the first identifier, the second identifier and the signal characteristics to determine the location of the first entity.

6. The method of claim 4, wherein the method further comprises:
receiving the first identifier using one or more additional wireless receivers associated with respective additional entities, said wireless receivers having respective identifiers;
pairing the first identifier, second identifier and the one or more additional identifiers; and
using the pairing to determine the location of the first entity.

7. The method of claim 6, further comprising:
determining signal characteristics associated with each received identifier; and
using the signal characteristics together with the pairing to determine the location of the first entity.

8. The method of claim 4, further comprising:
repeating the method steps at regular intervals; and
updating the location of the first entity.

9. The method of claim 6, wherein the wireless receivers comprise directional receivers and the location of the first entity is determined using triangulation.

10. The method of claim 5, wherein the first entity is one of: a cage, a scanning device, an employee, one or more articles of value, a container, a trolley, or a banknote sorter.

11. The method of claim 4, wherein the step of retrieving information comprises:
determining whether the first entity is authorised to be paired with the second entity;
if not generating an alert.

12. The method of claim 4, wherein:
the first entity comprises an operator within the cash processing centre; and
the step of retrieving information comprises:
authenticating the operator using the first identifier.

13. The method of claim 12, wherein:
the second entity comprises a device for use in the cash processing centre;
and the step of retrieving information further comprises:
if the operator is authenticated, retrieving user data associated with the operator;
based on the user data, determining whether the operator is authorised to use the device.

14. The method of claim 13, wherein the step of retrieving information further comprises:
if the operator is authorised, allowing access to the device, if not, denying access to the device.

15. The method of claim 12, wherein if the operator is not authenticated and/or authorised an alert is generated.

16. The method of claim 13, wherein the device comprises one of: a banknote counter or sorter, a client computing device, or a handheld electronic device.

17. The method of claim 13, wherein the step of determining whether the operator is authorised to use the device further comprises:
determining whether the operator is authorised to use any further devices connected to the device; and
if so, allowing access to the authorised further devices.

18. The method of claim 1, wherein the wireless devices comprise radio frequency identification devices.

19. The method of claim 1, wherein the first entity belongs to a first group of entities and the second entity belongs to a second group of entities.

20. A system for providing information about plurality of entities within a cash processing centre comprising:
a first wireless device coupled to a first entity;
a second wireless device coupled to a second entity; and
a processor adapted to:
read data associated with both the first and second wireless devices;
pair data associated with both the first and second wireless devices; and
retrieve information concerning the relationship between the first entity and the second entity based on the pairing.

21. The system of claim 20, wherein:
the first entity comprises a container for storing articles of value; and
the second entity comprises storage means for one or more containers; the processor being further adapted to:
retrieve information comprising the cumulative properties of the articles stored on or within the second entity based on the pairing.

22. The system of claim 20, wherein the first entity comprises one or more articles of value; and
the second entity comprises a unit adapted to store articles of value;
the processor being further adapted to:
retrieve information indicating that the first entity is stored upon the second entity.

23. The system of claim 20, wherein:
the first wireless device comprises a wireless transmitter configured to transmit a first identifier;
the second wireless device comprises a wireless receiver having a second identifier; and
the processor being further adapted to:
read a first identifier received from the second wireless device, together with the second identifier of said device, and pair said identifiers.

24. The system of claim 23, wherein the processor is further adapted to:
receive signal characteristics associated with the received first identifier; and

process the first identifier, the second identifier and the signal characteristics to determine the location of the first entity.

25. The system of claim **24**, wherein the system further comprises:

one or more additional wireless receivers associated with respective additional entities, said wireless receivers having respective additional identifiers; and

the processor is further adapted to:

receive one or more copies of the first identifier as received by one or more of the additional wireless receivers, together with the additional identifiers of said receivers;

pair the first identifier, second identifier and the one or more additional identifiers; and

determine the location of the first entity using the pairing.

26. The system of claim **25**, wherein the processor is further adapted to:

receive signal characteristics from each wireless receiver; and

process the signal characteristics together with the pairing to determine the location of the first entity.

27. The system of claim **24**, wherein the processor is adapted to:

repeat the processing steps at regular intervals to dynamically update the location of the first entity.

28. The system of claim **24**, wherein the wireless receivers comprise directional receivers and the processor is adapted to determine the location of the first entity using triangulation.

29. The system of claim **24**, wherein the first entity is one of: a cage, a scanning device, an employee, one or more articles of value, a container, a trolley, or a banknote sorter.

30. The system of claim **23**, further comprising:

a database comprising authorisation data;

wherein the processor is adapted to:

access the database to determine whether the first entity is authorised to be paired with the second entity; and

if not generate an alert.

31. The system of claim **23**, wherein:

the first entity comprises an operator within the cash processing centre; the system further comprises a database comprising authentication data; and the processor is further adapted to access the database to authenticate the operator using the first identifier.

32. The system of claim **31**, wherein: the second entity comprises a device for use in the cash processing centre;

the database further comprises authorisation data;

and the processor is further adapted to:

retrieve authorisation data associated with the operator from the database if the operator is authenticated;

based on the authorisation data, determine whether the operator is authorised to use the device.

33. The system of claim **32**, wherein the processor is further adapted to:

allow access to the device if the operator is authorised, or deny access to the device if the operator is not authorised.

34. The system of claim **31**, wherein the processor is further adapted to generate an alert if the operator is not authenticated and/or authorised.

35. The system of claim **32**, wherein the device comprises one of: a banknote counter or sorter, a client computing device, or a handheld electronic device.

36. The system of claim **32**, wherein the system further comprises:

one or more further devices connectable to the second entity;

and the processor is further adapted to:

based on the authorisation data, determine whether the operator is authorised to use any of said further devices; and

allow access to any connected further devices if the operator is authorised.

37. The system of claim **20**, wherein the wireless devices comprise radio frequency identification devices.

38. The system of claim **20**, wherein the first entity belongs to a first group of entities and the second entity belongs to a second group of entities.

39. A storage unit for containers for use in a cash processing centre, the containers containing one or more articles of value, the storage unit comprising: a storage area for one or more containers,

the storage unit by comprising:

one or more wireless receivers coupled to the storage unit configured to wirelessly read data from a wireless identification device and output data accordingly;

wherein, in use, each container is coupled to a wireless identification device, the wireless identification device storing data associated with properties of the articles of value within the container; and

in use, the properties of any articles of value stored upon the storage unit may be retrieved by processing data output by the one or more wireless receivers devices.

40. A method of tracking articles of value within a cash processing centre comprising:

a. coupling one or more articles of value with a first wireless identification device;

b. coupling a unit adapted to store articles of value with a second wireless identification device;

c. reading data associated with both the first and second wireless devices; and

d. recording that the one or more articles of value are stored upon the unit based on the read data.

41. A system for authenticating a user within a cash processing centre comprising:

a first wireless device coupled to a device to be operated by the user;

a second wireless device coupled to the user for identification;

a processor adapted to: read data from the first wireless device comprising identification data received from the second wireless device;

using the identification data authenticate the user with regard to the device to be operated by a user.

42. The system of claim **41**, wherein the processor is further adapted to determine if the user is authorise to operate the device to be operated: if so allowing the user to operate the device, if not preventing the user from operating the device.

* * * * *