CONTAINER FOR DELIVERIES

Field of the Invention

[0001] The present invention relates to a container for deliveries such as parcels delivered to a customer's home.

Background

[0002] With the rise of online shopping there is an increase in the number of parcels being delivered to customers' homes. However, it common for customers to be absent when their parcels are delivered as most deliveries are made within standard working hours.

[0003] In the case of such a failed delivery, a parcel is typically returned to a warehouse for storing until a new delivery is attempted or arranged. This process involves additional expense (e.g. in connection with transportation, storage and administrative functions) and ultimately delays the delivery of the parcel to the customer.

[0004] A known system that tries to address the above problem comprises locker depositories that are provided in various locations in residential areas such that failed deliveries are placed in a locker that is nearest to a customer's home and the customer is sent an access code to enable him/her to retrieve his/her parcels in his/her own time. While this may result in the parcel being received by a customer sooner than it would under the traditional system above (which requires a subsequent delivery), this system is also relatively expensive due to the cost of providing and maintaining the locker depositories.

[0005] In another known system, the locker depositories described above are replaced by existing convenience stores that provide a service by storing failed deliveries for subsequent customer collection. However, in both of the above systems, the onus is placed on the customers to travel (either to the locker depository or the convenience store) to collect their parcels.

[0006] It is therefore an aim of the present invention to provide a container for deliveries that helps to ameliorate one or more of the above shortcomings.

Summary of the invention

[0007] In accordance with a first aspect of the invention there is provided a container for deliveries comprising:

a. a container body for accommodating a delivery therein;

b. a location lock for securing the container to an exterior of a customer's property or outdoor furniture; and

c. a content lock for securing a delivery within the container body;

d. wherein the location lock and/or content lock is configured to unlock upon receiving a wireless signal key from an electronic device.

[0008] Embodiments of the invention therefore provide a container that can be used to secure deliveries at a customer's home when the customer is not present to accept the delivery directly. Thus, embodiments of the invention will reduce the instance of delivery failures. If the delivery can be accommodated within the container and the container secured to an exterior of the customer's property or outdoor furniture, it will be possible to use the container to securely deposit the delivery at the customer's home. Accordingly, there will be time, effort and cost savings by eliminating the need to attempt the delivery again. The cost savings will arise from reduced transportation and fuel costs (to return the delivery to a warehouse and re-deliver at a subsequent time) and reduced administration regarding the failed delivery and rescheduling of a subsequent delivery attempt. Furthermore, the customer receives the delivery on the first attempt and is not required to travel to collect the delivery even if he/she is not present when the delivery is made.

[0009] Although the container may ideally be suited for securing to a door handle or door hinge of the property, the outdoor furniture may comprise any relatively large or heavy objects which would be difficult for a burglar to remove from the property in a

concealed manner. For example, the container may be secured to a chair, table, swing, playhouse, shoe-rack, shed, railing, letterbox or plant.

[0010] The container may comprise an identifier (e.g. in the form of a barcode, QR code or serial number) for tracking the use of the container and associated deliveries.

[0011] The location lock may be provided on a handle of the container. The handle may be configured to attach to (e.g. loop around) a portion of the exterior of the customer's property or outdoor furniture to secure the container thereto.

[0012] The content lock may be provided inside the container body and configured to prevent access to an interior of the container when in a locked configuration.

[0013] The location lock and content lock may be configured for independent unlocking upon receiving a wireless signal key from an electronic device. In other words, the location lock and content lock may only unlock when they receive the wireless signal key that is unique to them.

[0014] The wireless signal key may be provided in the form of a non-audible frequency (e.g. a near-band voice-band frequency). For example, the wireless signal key may be provided in a frequency band of approximately 20kHz to 22kHz.

[0015] The wireless signal key may only be operational for a pre-defined duration (e.g. 5-10 minutes).

[0016] The location lock and or content lock may be configured to scan for the wireless signal key. The scan may be performed continuously or periodically.

[0017] The wireless signal key may comprise a message index (or header), a message (e.g. key payload), and a mixer code (or 'salt') for use in verifying a subsequent key. The message index may indicate which lock the key is for (e.g. the location lock or the content lock). The message may comprise the key for unlocking the lock. The mixer code may be calculated using a unique number assigned to each lock as a multiplier in a pre-determined algorithm. Thus, the mixer code is effectively a random code that may be used as an additional input to a one-way function that generates a password or passphrase. The primary function of the mixer code may be to defend against a fraudulent attack.

[0018] The lock may be configured to use a last stored mixer code as input to a pre-defined algorithm to verify that the message/key is valid. If the message/key is determined to be valid, the lock may send a return message to the electronic device and may store the mixer code in a memory for use in verifying a subsequent key. However, if the message/key is determined to be invalid, the lock may not send a return message to the electronic device and may not store the mixer code in a memory for use in verifying a subsequent key.

[0019] Conveniently, the container may be reusable so that, once a customer is in possession of the container he/she can reuse it for subsequent deliveries when he/she is likely to be absent at the time of delivery.

[0020] The container may be constituted by a bag, pouch, box or other type of portable container.

[0021] The container may be collapsible for ease of storage and/or transportation.

[0022] The container may be waterproof to protect container contents from adverse weather conditions.

[0023] The container may be tamper-resistant to protect container contents from unauthorised access.

[0024] In accordance with a second aspect of the invention there is provided a lock for a container for deliveries, the lock comprising: an unlocking actuator configured to unlock the lock upon receiving a wireless signal key from an electronic device.

[0025] The wireless signal key may be provided in the form of a non-audible frequency (e.g. a near-band voice-band frequency). For example, the wireless signal key may be provided in a frequency band of approximately 20kHz to 22kHz.

[0026] The wireless signal key may only be operational for a pre-defined duration (e.g. 5-10 minutes).

[0027] The location lock and or content lock may be configured to scan for the wireless signal key. The scan may be performed continuously or periodically.

[0028] The wireless signal key may comprise a message index (or header), a message (e.g. key payload), and a mixer code (or 'salt') for use in verifying a subsequent key. The message index may indicate which lock the key is for (e.g. the location lock or the content lock). The message may comprise the key for unlocking the lock. The mixer code may be calculated using a unique number assigned to each lock as a multiplier in a pre-determined algorithm. Thus, the mixer code is effectively a random code that may be used as an additional input to a one-way function that generates a password or passphrase. The primary function of the mixer code may be to defend against a fraudulent attack.

[0029] The lock may be configured to use a last stored mixer code as input to a pre-defined algorithm to verify that the message/key is valid. If the message/key is determined to be valid, the lock may send a return message to the electronic device and may store the mixer code in a memory for use in verifying a subsequent key. However, if the message/key is determined to be invalid, the lock may not send a return message to the electronic device and may not store the mixer code in a memory for use in verifying a subsequent key.

[0030] The location lock and/or content lock of the first aspect of the invention may be in accordance with the lock of the second aspect of the invention.

[0031] In accordance with a third aspect of the invention there is provided a method for delivering a parcel to a customer when the customer is not present at a time of delivery and wherein a container for deliveries is secured to an exterior of a customer's property or outdoor furniture, the method comprising:

[0032] a delivery person using a content lock to secure the parcel within the container;

[0033] the delivery person communicating an identifier for the container and delivery details to a delivery management server; and

[0034] the delivery management server communicating the delivery to the customer and providing a wireless signal key to be used by the customer to unlock the content lock to provide access to the parcel.

[0035] The container for deliveries may be in accordance with the first aspect of the invention.

[0036] In some embodiments, for example, when the customer does not already possess a container for deliveries, the delivery person may provide the container and may secure it to the exterior of the customer's property or outdoor furniture.

[0037] In other embodiments, for example, when the customer already possesses a container for deliveries, the customer may provide the container and may secure it to the exterior of the customer's property or outdoor furniture.

[0038] The delivery details may comprise one or more of: an order number, delivery time, delivery date, and identification of the delivery person.

[0039] The container may be secured to an exterior of the customer's property or outdoor furniture by a location lock and the delivery management server may further communicate a wireless signal key to be used by the customer to unlock the location lock.

[0040] The delivery person may use a delivery application operating on an electronic device, for communication with the delivery management server.

[0041] Notably, the delivery person may be associated with a delivery/logistics company operating the delivery management server or may be associated with a third party delivery/logistics company.

[0042] The customer may use a customer application operating on an electronic device, for communication with the delivery management server.

[0043] The electronic device used by the delivery person and/or customer may be constituted by a mobile telephone (which may be a smartphone or feature-phone), tablet, laptop, personal digital assistant (PDA) or other mobile device.

[0044] In accordance with a fourth aspect of the invention there is provided a delivery management server comprising a processor configured to:

[0045] receive an identifier for a container for deliveries and delivery details from a delivery person;

[0046] generate a wireless signal key to be used by a customer to unlock the container to provide access to a delivery therein; and

[0047] communicate the delivery and the wireless signal key to the customer.

[0048] The wireless signal key may be generated using a real time clock (RTC) plus part of the wireless signal key last generated by the server.

[0049] The container may be secured to an exterior of the customer's property or outdoor furniture by a location lock and the delivery management server may further generate and communicate a wireless signal key to be used by the customer to unlock the location lock.

[0050] The delivery management server may be configured to authenticate the delivery person and/or customer prior to initiating or accepting communication with them.

[0051] The wireless signal key may be provided in the form of a non-audible frequency (e.g. a near-band voice-band frequency). For example, the wireless signal key may be provided in a frequency band of approximately 20kHz to 22kHz.

[0052] The wireless signal key may only be operational for a pre-defined duration (e.g. 5-10 minutes).

[0053] The location lock and or container lock may be configured to scan for the wireless signal key. The scan may be performed continuously or periodically.

[0054] The wireless signal key may comprise a message index (or header), a message (e.g. key payload), and a mixer code (or 'salt') for use in verifying a subsequent key. The message index may indicate which lock the key is for (e.g. the location lock or the container lock). The message may comprise the key for unlocking the lock. The mixer code may be calculated using a unique number assigned to each lock as a multiplier in a pre-determined algorithm. Thus, the mixer code is effectively a random code that may be used as an additional input to a one-way function that generates a password or passphrase. The primary function of the mixer code may be to defend against a fraudulent attack.

[0055] The lock may be configured to use a last stored mixer code as input to a pre-defined algorithm to verify that the message/key is valid. If the message/key is determined to be valid, the lock may send a return message to the electronic device and may store the mixer code in a memory for use in verifying a subsequent key.

However, if the message/key is determined to be invalid, the lock may not send a return message to the electronic device and may not store the mixer code in a memory for use in verifying a subsequent key.

Brief description of the drawings

[0056] Embodiments of the invention will now be described, by way of example only, with reference to the following drawings, in which:

[0057] Figure 1 shows a schematic diagram of an embodiment of the invention;

[0058] Figure 2A shows a flowchart of a general method for delivering a parcel to a customer when the customer is not present in accordance with an embodiment of the invention;

[0059] Figure 2B shows a flowchart of operation of a delivery management server in accordance with an embodiment of the invention;

[0060] Figure 3A shows a flowchart of a method for delivering a parcel to a customer when the customer is not present in accordance with a particular embodiment of the invention;

[0061] Figure 3B shows a flowchart illustrating operation of the delivery management server in relation to the method of Figure 3A;

[0062] Figure 4A shows a flowchart of a method for a customer to access a parcel delivered in accordance with Figure 3A;

[0063] Figure 4B shows a flowchart illustrating operation of the delivery management server in relation to the method of Figure 4A, when unlocking a container to access the parcel within;

[0064] Figure 4C shows a flowchart illustrating operation of the delivery management server in relation to the method of Figure 4A, when unlocking a location lock to remove the container from the customer's door handle;

[0065] Figure 5A shows a flowchart of a method for a customer to re-use a container according to an embodiment of the invention, when the customer is expecting a delivery in their absence;

[0066] Figure 5B shows a flowchart illustrating operation of the delivery management server in relation to the method of Figure 5A;

[0067] Figure 6A shows a flowchart of a method for a customer to unlock a container according to an embodiment of the invention, for re-use; and

[0068] Figure 6B shows a flowchart illustrating operation of the delivery management server in relation to the method of Figure 6A.

Detailed description of certain embodiments

[0069] In accordance with a first embodiment of the present invention there is provided a container 10 for deliveries, as illustrated in Figure 1. In particular, the container 10 comprises a container body in the form of a collapsible pouch or bag 12 for accommodating a delivery or parcel 14 therein; a content lock 16 for securing the parcel 14 within the pouch 12; and a location lock 18 provided on a handle 20 for securing the pouch 12 to an exterior of a customer's property, which in this case is constituted by a door handle 22 on a door 24. As will be explained in more detail below, both the content lock 16 and location lock 18 are configured to unlock upon receiving a wireless signal key 26 from an electronic device. As shown in Figure 1, the electronic device may be a delivery device 28 or customer device 30. In both cases, the electronic device is a smartphone although other devices may be used including feature-phones, tablets, laptops and PDAs.

[0070] As illustrated in Figure 1, the delivery device 28 and the customer device 30 are in communication with a delivery management server 32 through a communication network 34 (which may be a standard mobile telephone network).

[0071] The container 10 in the present embodiment includes an identifier 36 in the form of a barcode printed on the pouch 12. The container 10 is also made from waterproof and tamper-resistant materials such as a durable plastics material.

[0072] Figure 2A shows a flowchart of a general method 40 for delivering the parcel 14 to a customer when the customer is not present at a time of delivery and wherein a container 10 for deliveries such as that illustrated in Figure 1 is secured to an exterior of a customer's property or outdoor furniture in accordance with an embodiment of the invention. The method 50 comprises the following steps:

[0073] Step 42: a delivery person uses the content lock 16 to secure the parcel 14 within the pouch 12;

[0074] Step 44: the delivery person communicates the identifier for the container 10 and delivery details to the delivery management server 32; and

[0075] Step 46: the delivery management server 32 communicates the delivery to the customer and provides the wireless signal key 26 to be used by the customer to unlock the content lock 16 to provide access to the parcel 14.

[0076] As illustrated in Figure 2B, the delivery management server 32 comprises a processor configured to carry out the method 50 in the following steps in accordance with an embodiment of the invention:

[0077] Step 52: receive the identifier 36 for the container 10 and delivery details from a delivery person;

[0078] generate the wireless signal key 26 to be used by a customer to unlock the container 10 to provide access to the parcel 14 therein; and

[0079] communicate the delivery and the wireless signal key 26 to the customer.

[0080] It will be understood that communication between the delivery person and the delivery management server 32 will be made through the delivery device 28 using a delivery application. Furthermore, communication between the customer and the delivery management server 32 will be made through the customer device 30 using a customer application. However, in embodiments where either the delivery person or the customer is using a feature-phone as opposed to a smart-phone, tablet or laptop, the above communications may be made using a voice recognition system or human operator instead of an application.

[0081] Use of the container 10 described above will be described in more detail below in relation to various different examples. In these examples, the delivery person is referred is a delivery champ.

Example 1: Delivery attempted when customer is absent

[0082] In a first example, the customer is not at the delivery address to receive the delivery when the delivery champ arrives with the parcel 14 to be delivered. In order to avoid a so-called no-show or failed delivery, the delivery champ utilises the container 10 described above to securely deliver the parcel 14 to the customer.

[0083] In this example, it is assumed that the customer is not already in possession of the container 10 according to an embodiment of the invention and so the delivery person uses the container 10 that he/she brings with him/her on every attempted delivery in case it is required.

[0084] Figure 3A shows a flowchart A of the steps carried out in order to securely deliver the parcel 14 to the customer in this scenario. The scenario begins with the delivery champ at the customer's door 24 in step 60. The delivery champ selects an order number relating to the present delivery in the delivery application and scans the barcode identifier 36 (referred to simply as the barcode in the remainder of this description) on the pouch 12 for the container 10 that is to be used for this delivery in step 62. The order number and barcode are then communicated to the delivery management server 32 over the communication network 34. In step 64, the delivery management server 32 verifies the order number and barcode against a token identifying the delivery champ. This step is explained in more detail in Figure 3B.

[0085] In step 66, if the order number and barcode are deemed to be valid, the procedure proceeds to step 68. However, if the order number and barcode are not valid, the procedure returns to step 62 for the delivery champ to re-enter the relevant details.

[0086] In step 68, the server sends an unlock code to the delivery person through the delivery application. As described above, the unlock code is in the form of a wireless signal key 26 non-audible frequencies. In step 70, the delivery device 28 transmits the wireless signal key 26 to cause the content lock 16 of the container 10 to unlock and in step 72, the content lock 16 unlocks the pouch 12 of the container 10.

[0087] The wireless signal key 26 may comprise a message index (or header), a message (e.g. key payload), and a mixer code (or 'salt') for use in verifying a subsequent key. The message index may indicate which lock the key is for (e.g. the content lock 16). The message may comprise the key 26 for unlocking the lock 16. The mixer code may be calculated using a unique number assigned to each lock 16 as a multiplier in a pre-determined algorithm.

[0088] The content lock 16 may be configured to use a last stored mixer code as input to a pre-defined algorithm to verify that the message/key is valid. If the message/key is determined to be valid, the content lock 16 may send a return message to the delivery device 28 and may store the mixer code in a memory for use in verifying a subsequent key. However, if the message/key is determined to be invalid, the content lock 16 may not send a return message to the delivery device 28 and may not store the mixer code in a memory for use in verifying a subsequent key.

[0089] In step 74, the delivery champ places an order (e.g. the parcel 14) in the pouch 12 and closes and locks the pouch 12 shut. In step 76, the delivery champ hangs the pouch 12 on the door handle 22 on the customer door 24 using the container handle 20 and location lock 18 so that the container 10 (and parcel 14) cannot be removed from the customer's home without unlocking the location lock 18.

[0090] In step 78, the delivery champ confirms the delivery to the delivery management server 32 through the delivery application. Note, in this embodiment, it will not be possible for the delivery champ to open any further containers 10 until they have confirmed successful delivery of the present parcel 14.

[0091] In step 80, the delivery management server 32 sends an SMS message to the customer associated with the delivery to confirm the delivery and provide an authentication code and link that the customer may use to download the customer application if they do not already have it on the customer device 30.

[0092] Figure 3B shows a flowchart illustrating in more detail the operation of the delivery management server 32 in relation to the method of Figure 3A described above.

[0093] In particular, interaction between the delivery person and the delivery management server 32 requires an authentication process which begins in step 90 with the delivery person entering an ID (i.e. username) and password into the delivery

application. Note, in the scenario illustrated, the delivery person has already registered with the delivery management server 32 and their details are stored in a database. In step 92, the delivery application sends an access request to the delivery management server 32. The access request includes the ID and password entered by the delivery person in step 90. In step 94, the delivery management server 32 checks whether the ID and password are valid (i.e. whether they correspond with the details for a registered delivery person stored in the database). If the ID and password are not valid the delivery management server 32 relays a message to the delivery application and the delivery person is prompted to re-enter their ID and password. If the ID and password are valid the delivery management server 32 generates a token in step 96 and communicates the token to the delivery application. In step 98, the delivery application stores the token.

[0094] In step 100, the delivery person scans the barcode on the pouch 12 to be used for the present delivery. In step 102, the delivery application sends a request to the delivery management server 32 to unlock the pouch 12 associated with the barcode. The request includes the barcode and token. The delivery management server 32 then checks whether the barcode and token are valid in step 104. This may comprise checking whether the token matches the one sent to the delivery person when they logged into the delivery application in the process described above and whether the barcode matches one in a database listing currently unused containers 10 and their barcodes. If the token and/or barcode are deemed to be invalid, the delivery management server 32 relays a message to the delivery application and the delivery person is prompted to re-scan the barcode and/or re-register with the delivery management server 32. If the token and barcode are valid the delivery management server 32 generates an unlock code in step 106 and communicates the unlock code to the delivery application. In step 108, the delivery application converts the unlock code into a non-audible frequency and transmits the non-audible frequency (i.e. wireless signal key) to the container 10. In step 110, the content lock 16 receives the wireless signal key and unlocks allowing access to the contents of the pouch 12.

[0095] As above, the wireless signal key 26 may comprise a message index (or header), a message (e.g. key payload), and a mixer code (or 'salt') for use in verifying a subsequent key. The message index may indicate which lock the key is for (e.g. the content lock 16). The message may comprise the key 26 for unlocking the content lock

16. The mixer code may be calculated using a unique number assigned to each lock 16 as a multiplier in a pre-determined algorithm.

[0096] The content lock 16 may be configured to use a last stored mixer code as input to a pre-defined algorithm to verify that the message/key is valid. If the message/key is determined to be valid, the content lock 16 may send a return message to the delivery device 28 and may store the mixer code in a memory for use in verifying a subsequent key. However, if the message/key is determined to be invalid, the content lock 16 may not send a return message to the delivery device 28 and may not store the mixer code in a memory for use in verifying a subsequent key.

[0097] In step 112, the delivery champ is able to use the container 10 by placing the parcel 14 to be delivered inside the pouch 12 and closing the content lock 16 to secure the parcel 14 therein.

[0098] If, as in this example, the container 10 is being used for the first time (i.e. scanned through the delivery device 28 for the first time) both the location lock 18 and the content lock 16 will be unlocked using the above process.

[0099] However, as is described below in example 3, when the customer secures the container 10 outside his/her property and use of the container 10 is attempted for a subsequent delivery, only the content lock 16 will be opened using the above process and not the location lock 18, thereby ensuring that the container 10 remains secured to the property and no one can remove it.

[00100] In the present example, once the parcel 14 is secured in the pouch 12 and the location lock 18 is locked to secure the container 10 to the customer's door handle 22, the container 10 can only be opened and/or removed from the door handle 22 using the authentication code sent to the customer in step 80. It should be noted that although, in this example, the authentication code is sent via SMS, in other embodiments, the authentication code may be relayed via other means such as by email.

[00101] The unlocking of the container 10 by the customer is described in detail below in relation to example 2.

Example 2: Customer returns to find container at his/her door

[00102] In example 2, the customer returns home and finds the container 10 attached to their door handle 22, with the parcel 14 locked inside.

[00103] Figure 4A shows a flowchart of a method B for the customer to access the parcel 14 that has been delivered in accordance with Figures 3A and 3B. This example begins in step 120 with the customer being at home and close to the container 10 locked to the door 24.

[00104] The customer opens the customer application on the customer device 30 and selects the order number for the delivery in the step 122. The customer is then prompted to choose whether they wish to unlock content lock 16 (i.e. pouch lock) for access to the parcel 14 inside the pouch 12 or the location lock 18 on the handle 20 (i.e. handle lock) to remove the container 10 from the door 24. In step 124, the customer selects the lock (i.e. pouch or handle) that they wish to open.

[00105] If they customer selects to unlock the pouch 12, in step 126 the application will ask the customer to input the authentication code provided to them by the delivery management server 32 in step 80. In step 128, the customer inputs the authentication code into the customer application which then sends it to the delivery management server 32 for validation. In step 130, the delivery management server 32 checks whether the authentication code matches the order number and, if not, the process returns to step 126 for the customer to re-enter the authorization code. If the authorization code is correct, in step 132, the delivery management server 32 sends a wireless signal key 26 for unlocking the pouch 12 to the customer application. In step 134, the customer application transmits the wireless signal key 26 from the customer device 30 to the content lock 16 in a non-audible frequency and in step 136 the content lock 16 accepts the wireless signal key 26 and unlocks the pouch 12 to allow the customer to retrieve the parcel 14 within.

[00106] As above, the wireless signal key 26 may comprise a message index (or header), a message (e.g. key payload), and a mixer code (or 'salt') for use in verifying a subsequent key. The message index may indicate which lock the key is for (e.g. the content lock 16). The message may comprise the key 26 for unlocking the content lock 16. The mixer code may be calculated using a unique number assigned to each lock 16 as a multiplier in a pre-determined algorithm.

[00107] The content lock 16 may be configured to use a last stored mixer code as input to a pre-defined algorithm to verify that the message/key is valid. If the message/key is determined to be valid, the content lock 16 may send a return message to the customer device 30 and may store the mixer code in a memory for use in verifying a subsequent key. However, if the message/key is determined to be invalid, the content lock 16 may not send a return message to the customer device 30 and may not store the mixer code in a memory for use in verifying a subsequent key.

[00108] In step 138, the customer will decide whether to also unlock the location lock 18 on the handle 20 so that the container 10 can be removed from the door 24. If the customer does not wish to remove the container 10, the process will end. However, if the customer does wish to unlock the location lock 18, process flow B1 will be initiated for carrying out the request for unlocking the handle 20. This is the same process that will result if the customer chooses in step 124 to unlock the handle 20 as opposed to the pouch 12.

[00109] This flow begins in step 140, with the customer application communicating with the delivery management server 32 to check whether the pouch 12 is already unlocked. If the pouch is not currently unlocked, in step 142, the customer application will ask the customer to input their authentication code sent to them in step 80 above. In step 144 the customer will input the authentication code to the customer application which will send the authentication code to the delivery management server 32. In step 146, the delivery management server 32 will check with the authorization code is valid by checking it against the order number selected previously in step 122. If the authentication code is not valid, the process will return to step 142 for the customer to re-enter the authentication code. If the authentication code is valid, the process will continue with step 148 in which the delivery management server 32 sends the wireless signal key 26 for the location lock 18 to the customer application.

[00110] Note that if the pouch 12 was determined in step 140 to be already open, the process flow would jump immediately to step 148 without requiring the customer to re-enter the authentication code. Thus, it will be noted that in this embodiment the authentication code is always required to be entered for the content lock 16 to be opened so that the customer can access the parcel 14 in the pouch 12. However, the authentication code will only be required to be entered to unlock the location lock 18 to

open the handle 20 to remove the container 10 from the door 24 if the pouch 12 is still locked.

[00111] Once the customer application receives the wireless signal key 26 for the location lock 18, it transmits the wireless signal key 26 in a non-audible frequency from the customer device 30 to the location lock 18 in step 150. The location lock 18 will then unlock in step 152.

[00112] As above, the wireless signal key 26 may comprise a message index (or header), a message (e.g. key payload), and a mixer code (or 'salt') for use in verifying a subsequent key. The message index may indicate which lock the key is for (e.g. the location lock 18). The message may comprise the key 26 for unlocking the location lock 18. The mixer code may be calculated using a unique number assigned to each lock 18 as a multiplier in a pre-determined algorithm.

[00113] The location lock 18 may be configured to use a last stored mixer code as input to a pre-defined algorithm to verify that the message/key is valid. If the message/key is determined to be valid, the location lock 18 may send a return message to the customer device 30 and may store the mixer code in a memory for use in verifying a subsequent key. However, if the message/key is determined to be invalid, the location lock 18 may not send a return message to the customer device 30 and may not store the mixer code in a memory for use in verifying a subsequent key.

[00114] Finally, in step 154, the customer decides whether they now wish to unlock the pouch 12 (e.g. if this was not already done previously). If they do not wish to unlock the pouch 12 the process flow ends and if they do wish to unlock the pouch 12 the process flow returns to B1 for carrying out the request to unlock the pouch 12.

[00115] Figure 4B shows a flowchart illustrating in more detail the operation of the delivery management server 32 in relation to the method of Figure 4A, when unlocking the content lock 16 of the container 10 to access the parcel 14 within the pouch 12.

[00116] In step 160 the customer selects the order number for the delivery using the customer application. In step 162 the customer selects to unlock the pouch 12 using the customer application. In step 164, the customer application asks the customer to input the authentication code provided to them by the delivery management server 32 in previous step 80. The customer then inputs the authentication code in step 166 and

in step 168 the customer application sends a request to the delivery management server 32 for the wireless signal key 26 to unlock the pouch 12. The request includes the order number and authentication code. In step 170, the delivery management server 32 checks whether the authentication code is valid by comparing it with the order number and authentication code sent to the customer that is stored in a database. If the authentication code is invalid, the process returns to step 164 for the customer to re-enter the authentication code. If the authentication code is valid, the process moves to step 172 and the delivery management server 32 generates the wireless signal key 26 (i.e. unlock code) to unlock the pouch 12. The unlock code is then relayed to the customer application and in step 174 the customer application converts the unlock code into a non-audible frequency wireless signal key 26 which is transmitted via the customer device 30 to the pouch 12. The content lock 16 receives the wireless signal key 26 in step 176 and locks the pouch 12.

[00117] As above, the wireless signal key 26 may comprise a message index (or header), a message (e.g. key payload), and a mixer code (or 'salt') for use in verifying a subsequent key. The message index may indicate which lock the key is for (e.g. the content lock 16). The message may comprise the key 26 for unlocking the content lock 16. The mixer code may be calculated using a unique number assigned to each lock 16 as a multiplier in a pre-determined algorithm.

[00118] The content lock 16 may be configured to use a last stored mixer code as input to a pre-defined algorithm to verify that the message/key is valid. If the message/key is determined to be valid, the content lock 16 may send a return message to the customer device 30 and may store the mixer code in a memory for use in verifying a subsequent key. However, if the message/key is determined to be invalid, the content lock 16 may not send a return message to the customer device 30 and may not store the mixer code in a memory for use in verifying a subsequent key.

[00119] In step 178 the customer removes the parcel 12 from the pouch 14 and the delivery is complete.

[00120] Figure 4C shows a flowchart illustrating in more detail the operation of the delivery management server in relation to the method of Figure 4A, when unlocking the location lock 18 to remove the container 10 from the customer's door handle 20.

[00121] In step 180 the customer selects the order number for the delivery using the customer application. In step 182 the customer selects to unlock the location lock 18 on the handle 20 using the customer application. In step 184, the delivery management server 32 checks whether the pouch 12 is already unlocked. If the pouch 12 is not unlocked the process proceeds with step 186 and where customer application asks the customer to input the authentication code provided to them by the delivery management server 32 in previous step 80. The customer then inputs the authentication code in step 188 and in step 190 the customer application sends a request to the delivery management server 32 for the wireless signal key 26 to unlock the handle 20. The request includes the order number and authentication code. In step 192, the delivery management server 32 checks whether the authentication code is valid by comparing it with the order number and authentication code sent to the customer and that is stored in a database. If the authentication code is invalid, the process returns to step 186 for the customer to re-enter the authentication code. If the authentication code is valid, the process moves to step 194 and the delivery management server 32 generates the wireless signal key 26 (i.e. unlock code) to unlock the handle 20. The unlock code is then relayed to the customer application and in step 196 the customer application converts the unlock code into a non-audible frequency wireless signal key 26 which is transmitted via the customer device 30 to the location lock 18 on the handle 20. The location lock 18 receives the wireless signal; key 26 in step 198 and unlocks the handle 20.

[00122] As above, the wireless signal key 26 may comprise a message index (or header), a message (e.g. key payload), and a mixer code (or 'salt') for use in verifying a subsequent key. The message index may indicate which lock the key is for (e.g. the location lock 18). The message may comprise the key 26 for unlocking the location lock 18. The mixer code may be calculated using a unique number assigned to each lock 18 as a multiplier in a pre-determined algorithm.

[00123] The location lock 18 may be configured to use a last stored mixer code as input to a pre-defined algorithm to verify that the message/key is valid. If the message/key is determined to be valid, the location lock 18 may send a return message to the customer device 30 and may store the mixer code in a memory for use in verifying a subsequent key. However, if the message/key is determined to be invalid,

the location lock 18 may not send a return message to the customer device 30 and may not store the mixer code in a memory for use in verifying a subsequent key.

[00124] In step 200 the customer removes the container 10 from the door handle 22.

[00125] As mentioned above, if the pouch is already unlocked in step 184, the process flow jumps straight to step 194 for the generation of the wireless signal key 26 without requiring the authentication process described above to be repeated.

[00126] In the current example the customer has unlocked the pouch 12 and retrieved the delivered parcel 14 and removed the container 10 from the door handle 22 by unlocking the location lock 18. Accordingly, the delivery is complete and the customer may retain the container 10 for future use as described below in relation to example 3.

Example 3: Customer uses container for future deliveries

[00127] If the customer is already in possession of the container 10, he/she can reuse the container 10 for accepting future deliveries if the/she is expecting a delivery when he/she is not going to be present at the delivery address.

[00128] Notably, in the present example, the container 10 may be used by a delivery person associated with a delivery company that provided the container 10 (e.g. as in the process described above in relation to Figure 3B) and/or that operates the delivery management server 32 or another delivery company unrelated to the above.

[00129] Figure 5A shows a flowchart of a method C for a customer to re-use the container 10 according to an embodiment of the invention, when the customer is expecting a delivery in their absence. The method C begins in step 210 with the customer wishing to receive a delivery using the container 10 already in his/her possession.

[00130] In step 212, the customer checks whether the container 10 is locked. This includes checking whether the pouch 12 is locked with the content lock 16 and whether the handle 20 is locked by the location lock 18. If either of the content lock 16 or location lock 18 are locked, the customer must first unlock the locks by carrying out process flow D which is described below in relation to Figures 6A and 6B. In the

present example, it is assumed that both lock are unlocked in step 212 and so the process flow passes to step 214.

[00131] In step 214 the customer attaches the container 10 to the exterior of his/her house or outside furniture. In this case, the customer hangs the container 10 on the his/her door handle 22 by looping the handle 20 of the container 10 around the door handle 22 and locking the location lock 18 to secure the container 10 in place. The customer also locks the content lock 16 to seal the pouch 12 before leaving the property.

[00132] In step 216, the delivery champ arrives at the customer's door 24 to deliver the parcel 14 and the customer is not present. In step 218, the delivery champ will login to the delivery application in accordance with the process flow described in steps 90 to 98 in relation to Figure 3B. It should be understood that, if the delivery champ does not already have the delivery application on his/her delivery device 28, he/she may download the delivery application and register with the delivery management server 32 before logging in to the delivery application as described above. Once logged in, the delivery champ will enter an order number, scan the pouch barcode and send a request to the delivery management server 32 to unlock the content lock 16 for the pouch 12. In step 220, the delivery management server 32 will verify the order number, barcode (i.e. pouch number) and token for the delivery champ (i.e. champ validity number) as issued during the login process. In step 222, if at least one of the order number, barcode and token are not valid the process will return to step 218 for re-entry of the relevant details. On the other hand, if the order number, barcode and token are valid the process will proceed to step 224 where the delivery management server 32 will check against database records to determine whether the container 10 is already occupied with a parcel 12 or if it is empty. If the container 10 is occupied, the delivery management server 32 will send a message to the delivery application to inform the delivery champ that the container 10 is already in use and the delivery champ will have the option of using a new container 10 for the present delivery, in step 232. In this case, process flow A will proceed as described above in relation to Figures 3A and 3B.

[00133] If the container 10 is determined to be unoccupied the process continues with step 226 and the delivery management server 32 sends an unlock code to the delivery application for the content lock 16 to unlock the pouch 12. In step 228, the delivery

application transmits the unlock code in the form of a non-audible frequency wireless signal key 26 to the content lock 16 and in step 230 the pouch 12 unlocks.

[00134] As above, the wireless signal key 26 may comprise a message index (or header), a message (e.g. key payload), and a mixer code (or 'salt') for use in verifying a subsequent key. The message index may indicate which lock the key is for (e.g. the content lock 16). The message may comprise the key 26 for unlocking the content lock 16. The mixer code may be calculated using a unique number assigned to each lock 16 as a multiplier in a pre-determined algorithm.

[00135] The content lock 16 may be configured to use a last stored mixer code as input to a pre-defined algorithm to verify that the message/key is valid. If the message/key is determined to be valid, the content lock 16 may send a return message to the customer device 30 and may store the mixer code in a memory for use in verifying a subsequent key. However, if the message/key is determined to be invalid, the content lock 16 may not send a return message to the customer device 30 and may not store the mixer code in a memory for use in verifying a subsequent key.

[00136] The process then proceeds in accordance with the flow labelled A1 in Figure 3A.

[00137] Figure 5B shows a flowchart illustrating in more detail the operation of the delivery management server 32 in relation to the method of Figure 5A.

[00138] As explained above, the delivery champ must first login to the delivery application using the process flow shown in steps 240 to 248. As before, in this example, it is assumed that the delivery person has already registered with the delivery management server 32 and their details are stored in a database. In step 240 the delivery person enters an ID (i.e. username) and password into the delivery application. In step 242 the delivery application sends an access request to the delivery management server 32. The access request includes the ID and password entered by the delivery person in step 240. In step 244, the delivery management server 32 checks whether the ID and password are valid (i.e. whether they correspond with the details for a registered delivery person stored in the database). If the ID and password are not valid the delivery management server 32 relays a message to the delivery application and the delivery person is prompted to re-enter their ID and password. If

the ID and password are valid the delivery management server 32 generates a token in step 246 and communicates the token to the delivery application. In step 248, the delivery application stores the token.

[00139] In step 250, the delivery person scans the barcode on the pouch 12 to be used for the present delivery. In step 252, the delivery application sends a request to the delivery management server 32 to unlock the pouch 12 associated with the barcode. The request includes the barcode and token. The delivery management server 32 then checks whether the barcode and token are valid in step 254. This may comprise checking whether the token matches the one sent to the delivery person when they logged into the delivery application in the process described above and whether the barcode matches one in a database listing currently unused containers 10 and their barcodes. If the token and/or barcode are deemed to be invalid, the delivery management server 32 relays a message to the delivery application and the delivery person is prompted to re-scan the barcode and/or re-register with the delivery management server 32. If the token and barcode are valid the delivery management server 32 checks, in step 256, whether the pouch 12 is empty by checking a status of the pouch 12 as stored in a database. If the pouch 12 is occupied with a parcel 14, in step 258, the delivery champ is informed (via the delivery application) that the pouch 12 cannot be used and the delivery champ has the option of using a new container in accordance with process flow A described above.

[00140] If the pouch 12 is empty, the delivery management server 32 generates an unlock code in step 260 and communicates the unlock code to the delivery application. In step 262, the delivery application converts the unlock code into a non-audible frequency and transmits the non-audible frequency (i.e. wireless signal key) to the container 10. In step 264, the content lock 16 receives the wireless signal key and unlocks allowing access to the contents of the pouch 12.

[00141] As above, the wireless signal key 26 may comprise a message index (or header), a message (e.g. key payload), and a mixer code (or 'salt') for use in verifying a subsequent key. The message index may indicate which lock the key is for (e.g. the content lock 16). The message may comprise the key 26 for unlocking the content lock 16. The mixer code may be calculated using a unique number assigned to each lock 16 as a multiplier in a pre-determined algorithm.

[00142] The content lock 16 may be configured to use a last stored mixer code as input to a pre-defined algorithm to verify that the message/key is valid. If the message/key is determined to be valid, the content lock 16 may send a return message to the customer device 30 and may store the mixer code in a memory for use in verifying a subsequent key. However, if the message/key is determined to be invalid, the content lock 16 may not send a return message to the customer device 30 and may not store the mixer code in a memory for use in verifying a subsequent key.

[00143] In step 268, the delivery champ is able to use the container 10 by placing the parcel 14 to be delivered inside the pouch 12 and closing the content lock 16 to secure the parcel 14 therein.

[00144] As mentioned above, if the container 10 is already locked when the customer decides to reuse it, the process flow D explained below in example 4 is first carried out to unlock the container 10 ready for subsequent use.

Example 4: Customer unlocks container for re-use

[00145] In this example, the customer wishes to use an existing container 10 but needs to open the content lock 16 and location lock 18 so that the container 10 can be reused. The customer may have locked one or both of the content lock 16 and location lock 18 after retrieving an earlier delivery, as described above.

[00146] Figure 6A shows a flowchart of a method D for the customer to unlock the container 10 according to an embodiment of the invention, for re-use. In step 270 the customer scans the pouch 12 barcode using his/her customer device 30 and makes a request to the delivery management server 32, through the customer application, for an unlock code to unlock the container 10 (including pouch 12 and handle 20).

[00147] In step 272 the delivery management server 32 verifies with a database the pouch barcode and token that was issued to the customer when the customer logged into the customer application. This customer login process is described in more detail below in relation to Figure 6B. In step 274, if the token or barcode are invalid the process returns to step 270 for the customer to re-enter the barcode. Although not shown, the customer may also be requested to login to the customer application again to refresh the token.

[00148] If the token and barcode are valid the process proceeds with step 276 where the delivery management server 32 generates and sends the unlock codes for each of the content lock 16 and location lock 18 to the customer application. In step 278 the customer application transmits the unlock codes (i.e. wireless signal keys) in an non-audible frequency from the customer device 30 to the pouch 12 and in step 280 the pouch 12 and handle 20 are unlocked as the content lock 16 and location lock 18 are configured to both unlock upon receiving their respective wireless signal keys 26.

[00149] As above, each of the wireless signal keys 26 may comprise a message index (or header), a message (e.g. key payload), and a mixer code (or 'salt') for use in verifying a subsequent key. The message index may indicate which lock the key is for (e.g. the content lock 16 or location lock 18). The message may comprise the key 26 for unlocking the content lock 16 or location lock 18. The mixer code may be calculated using a unique number assigned to each lock 16, 18 as a multiplier in a pre-determined algorithm.

[00150] The content lock 16 or location lock 18 may be configured to use a last stored mixer code as input to a pre-defined algorithm to verify that the message/key is valid. If the message/key is determined to be valid, the content lock 16 or location lock 18 may send a return message to the customer device 30 and may store the mixer code in a memory for use in verifying a subsequent key. However, if the message/key is determined to be invalid, the content lock 16 or location lock 18 may not send a return message to the customer device 30 and may not store the mixer code in a memory for use in verifying a subsequent key.

[00151] Figure 6B shows a flowchart illustrating in more detail the operation of the delivery management server 32 in relation to the method of Figure 6A.

[00152] As explained above, the customer must first login to the customer application. This process is identical to that described above in relation to the delivery champs logging into the delivery application. However, for completeness, the customer process flow is shown in steps 290 to 298. As before, in this example, it is assumed that the customer has already registered with the delivery management server 32 and their details are stored in a database. In step 290 the customer enters an ID (i.e. username) and password into the customer application. In step 292 the customer application sends an access request to the delivery management server 32. The access request

includes the ID and password entered by the customer in step 290. In step 294, the delivery management server 32 checks whether the ID and password are valid (i.e. whether they correspond with the details for a registered customer stored in the database). If the ID and password are not valid the delivery management server 32 relays a message to the customer application and the customer is prompted to re-enter their ID and password. If the ID and password are valid the delivery management server 32 generates a token in step 296 and communicates the token to the customer application. In step 298, the customer application stores the token for future use.

[00153] In step 300, the customer scans the barcode on the pouch 12 to be used for the present delivery. In step 302, the customer application sends a request to the delivery management server 32 for an unlock code to unlock both the pouch 12 and the handle 20 associated with the barcode. The request includes the barcode and token for the customer as stored in step 298. The delivery management server 32 then checks whether the barcode and token are valid in step 304. This may comprise checking whether the token matches the one sent to the customer when they logged into the customer application in the process described above and whether the barcode matches one in a database listing currently unused containers 10 and their barcodes. If the token and/or barcode are deemed to be invalid, the delivery management server 32 relays a message to the customer application and the customer is prompted to re-scan the barcode and/or re-register with the delivery management server 32. If the token and barcode are valid the delivery management server 32 generates unlock codes in step 306 and communicates the unlock codes to the customer application. In step 308, the customer application converts the unlock codes into a non-audible frequency and transmits the non-audible frequency (i.e. wireless signal keys) to the container 10. In step 310, the content lock 16 and location lock 18 receive their respective wireless signal keys 26 and unlock allowing access to the pouch 12 and opening of the handle 20 so it can be re-hung on the customer's door 24.

[00154] As above, each of the wireless signal keys 26 may comprise a message index (or header), a message (e.g. key payload), and a mixer code (or 'salt') for use in verifying a subsequent key. The message index may indicate which lock the key is for (e.g. the content lock 16 or location lock 18). The message may comprise the key 26 for unlocking the content lock 16 or location lock 18. The mixer code may be

calculated using a unique number assigned to each lock 16, 18 as a multiplier in a pre-determined algorithm.

[00155] The content lock 16 or location lock 18 may be configured to use a last stored mixer code as input to a pre-defined algorithm to verify that the message/key is valid. If the message/key is determined to be valid, the content lock 16 or location lock 18 may send a return message to the customer device 30 and may store the mixer code in a memory for use in verifying a subsequent key. However, if the message/key is determined to be invalid, the content lock 16 or location lock 18 may not send a return message to the customer device 30 and may not store the mixer code in a memory for use in verifying a subsequent key.

[00156] In step 312, the customer is able to re-use the container 10 for receipt of future deliveries by following process C described above in relation to Figures 5A and 5B.

[00157] Although only certain embodiments of the present invention have been described in detail, many variations are possible in accordance with the appended claims.

Claims

1. A container for deliveries comprising:

a container body for accommodating a delivery therein;

a location lock for securing the container to an exterior of a customer's property or outdoor furniture; and

a content lock for securing a delivery within the container body;

wherein the location lock and/or content lock is configured to unlock upon receiving a wireless signal key from an electronic device.

2. The container according to claim 1 wherein the container comprises an identifier for tracking the use of the container and associated deliveries.

3. The container according to either preceding claim wherein the location lock is provided on a handle of the container.

4. The container according to claim 3 wherein the handle is configured to attach to a portion of the exterior of the customer's property or outdoor furniture to secure the container thereto.

5. The container according to any preceding claim wherein the content lock is provided inside the container body and is configured to prevent access to an interior of the container when in a locked configuration.

6. The container according to any preceding claim wherein the location lock and content lock are configured for independent unlocking upon receiving a wireless signal key from an electronic device.

7. The container according to any preceding claim wherein the wireless signal key is provided in the form of a non-audible frequency

8. The container according to any preceding claim wherein the wireless signal key is only operational for a pre-defined duration.

9. The container according to any preceding claim wherein the container is reusable.

10. The container according to any preceding claim wherein the container is constituted by a bag, pouch, box or other type of portable container.

11. The container according to any preceding claim wherein the container is collapsible for ease of storage and/or transportation.

12. The container according to any preceding claim wherein the container is waterproof to protect container contents from adverse weather conditions.

13. The container according to any preceding claim wherein the container is tamper-resistant to protect container contents from unauthorised access.

14. A lock for a container for deliveries, the lock comprising:

an unlocking actuator configured to unlock the lock upon receiving a wireless signal key from an electronic device.

15. The lock according to claim 14 wherein the wireless signal key is provided in the form of a non-audible frequency.

16. The lock according to claim 14 or claim 15 wherein the wireless signal key is only operational for a pre-defined duration.

17. A method for delivering a parcel to a customer when the customer is not present at a time of delivery and wherein a container for deliveries is secured to an exterior of a customer's property or outdoor furniture, the method comprising:

a) a delivery person using a content lock to secure the parcel within the container;

b) the delivery person communicating an identifier for the container and delivery details to a delivery management server; and

c) the delivery management server communicating the delivery to the customer and providing a wireless signal key to be used by the customer to unlock the content lock to provide access to the parcel.

18. The method according to claim 17 wherein the container for deliveries is in accordance with the container of any one of claims 1 to 13.

19. The method according to claim 17 or 18 wherein the delivery person provides the container and secures it to the exterior of the customer's property or outdoor furniture.

20. The method according to claim 17 or claim 18 wherein the customer provides the container and secures it to the exterior of the customer's property or outdoor furniture.

21. The method according to any one of claims 17 to 20 wherein the delivery details comprise one or more of: an order number, delivery time, delivery date, and identification of the delivery person.

22. The method according to any one of claims 17 to 21 wherein the container is secured to an exterior of the customer's property or outdoor furniture by a location lock and the delivery management server further communicates a wireless signal key to be used by the customer to unlock the location lock.

23. The method according to any one of claims 17 to 22 wherein the delivery person uses a delivery application operating on an electronic device, for communication with the delivery management server.

24. The method according to any one of claims 17 to 23 wherein the customer uses a customer application operating on an electronic device, for communication with the delivery management server.

25. The method according to either one of claims 23 or 24 wherein the electronic device used by the delivery person and/or customer is constituted by a mobile telephone, tablet, laptop, PDA or other mobile device.

26. A delivery management server comprising a processor configured to:

a) receive an identifier for a container for deliveries and delivery details from a delivery person;

b) generate a wireless signal key to be used by a customer to unlock the container to provide access to a delivery therein; and

c) communicate the delivery and the wireless signal key to the customer.

27. The delivery management server according to claim 26 wherein the wireless signal key is generated using a real time clock (RTC) plus part of the wireless signal key last generated by the delivery management server.

28. The delivery management server according to claim 26 or claim 27 wherein the container is secured to an exterior of the customer's property or outdoor furniture by a location lock and the delivery management server further generates and communicates a wireless signal key to be used by the customer to unlock the location lock.

29. The delivery management server according to any one of claims 26 to 28 further configured to authenticate the delivery person and/or customer prior to initiating or accepting communication with them.

30. The delivery management server according to any one of claims 26 to 29 wherein the wireless signal key is provided in the form of a non-audible frequency.

31. The delivery management server according to any one of claims 26 to 30 wherein the wireless signal key is only operational for a pre-defined duration.