

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7624801号
(P7624801)

(45)発行日 令和7年1月31日(2025.1.31)

(24)登録日 令和7年1月23日(2025.1.23)

(51)国際特許分類

F I

G 0 6 F 21/35 (2013.01)

G 0 6 F 21/44 (2013.01)

G 0 6 F 21/33 (2013.01)

G 0 6 F 21/35

G 0 6 F 21/44

G 0 6 F 21/33

請求項の数 20 外国語出願 (全32頁)

(21)出願番号	特願2019-227509(P2019-227509)	(73)特許権者	517352371
(22)出願日	令和1年12月17日(2019.12.17)		クアディエント・テクノロジー・フラン
(65)公開番号	特開2020-115329(P2020-115329 A)		ス
(43)公開日	令和2年7月30日(2020.7.30)		フランス・9 2 2 2 0・パニユー・アヴ
審査請求日	令和4年12月5日(2022.12.5)		ニュ・アリスティッド・ブリアン・4 2
(31)優先権主張番号	18306731.3	(74)代理人	100108453
(32)優先日	平成30年12月18日(2018.12.18)		弁理士 村山 靖彦
(33)優先権主張国・地域又は機関	欧州特許庁(EP)	(74)代理人	100110364
			弁理士 実広 信哉
		(74)代理人	100133400
			弁理士 阿部 達彦
		(72)発明者	ガブリエル・サンタンジュリ
			フランス・9 1 6 0 0・サヴィニーニ
			ユルーオルジュ・アヴニユー・ラウル・ル
			最終頁に続く

(54)【発明の名称】 区画の自律クラスタを備えた安全にされた小荷物ロッカーシステム

(57)【特許請求の範囲】
【請求項1】

少なくとも1つの区画(112j)を含むとともにロックモジュール(120i)を含む少なくとも1つの自律区画クラスタ(110i)で構成される少なくとも1つの小荷物ロッカー(100)を、長距離通信ネットワーク(104)を介してリモート配送システム(106)と通信する少なくとも1つのモバイルデバイス(102)を介して操作するための方法であって、前記ロックモジュールは、エネルギー管理モジュール(230)と、アンテナ(218)を備えた無線トランシーバモジュール(216)と、を備え、前記エネルギー管理モジュール(230)は、エネルギーモードの移行を管理し、前記少なくとも1つの自律区画クラスタをスリープモードで動作させることを可能にするように構成され、前記方法は、

前記少なくとも1つのモバイルデバイスと前記リモート配送システムとの間の通信セッションを確立するステップと、

スリープモード中に、前記少なくとも1つのモバイルデバイスとの短距離通信セッションを確立するために、前記ロックモジュールにより、前記少なくとも1つのモバイルデバイスに宛てられたブロードキャストされたショートメッセージを定期的に発するステップと、

前記少なくとも1つのモバイルデバイスにより、前記リモート配送システムから、前記リモート配送システムによって生成され、前記少なくとも1つのモバイルデバイスに暗号化された形式で提供された認証子(300)を受信するステップであって、この認証子が、前記少なくとも1つのモバイルデバイスによって、前記認証子を含む要求を前記ロックモジ

ジュールに送信するために使用され、前記認証子が、区画インデックス(310)、前記ロックモジュールに関するユーザ権利を定義する特権マスク(312)、有効期限(314)、および一意の認証子識別情報(316)を含む、ステップと、

前記ロックモジュールに記憶されたシークレットキー(254)を用いて、前記要求の自動検証のために前記認証子を解読するステップであって、認証コードは生成されず、前記要求の前記自動検証のために前記ロックモジュールに提供されず、前記認証コードが、小荷物の受取人によって1回のみ使用することができるワンタイムコードである、ステップと、

を含み、前記スリープモード中に、前記ロックモジュール(120i)は、ショートメッセージをブロードキャストするために部分的に起動され、前記無線トランシーバモジュール(216)は、アクティブ化され、前記エネルギー管理モジュール(230)によって制御される、方法。

10

【請求項2】

前記認証子が一意または実質的に一意であり、前記ロックモジュールに関連付けられ前記シークレットキー(254)と一致するクラスタシークレットキー(136i)で暗号化され、前記クラスタシークレットキーが一意であり、前記ロックモジュールに一意に関連付けられることを特徴とする、請求項1に記載の方法。

【請求項3】

前記自動検証が、前記解読に続いて前記認証子の形式および内容を検証することによって実行され、または前記自動検証が、前記認証子に含まれる暗号ソルトを識別することによって実行され、または前記自動検証が、前記認証子に添付された署名を、解読後に前記認証子に基づいて前記ロックモジュールにインストールされた暗号アルゴリズムによって計算された署名と比較することによって実行され、前記署名がハッシュであることを特徴とする、請求項1または2に記載の方法。

20

【請求項4】

前記要求が、前記認証子の有効期限(314)に達したかどうかをチェックすることによってさらに検証され、前記有効期限に達した場合、前記要求は許可されず、結果として、前記ロックモジュールと前記少なくとも1つのモバイルデバイスとの間の切断となり、前記有効期限が、前記少なくとも1つの小荷物ロッカーのユーザカテゴリーに依存する前記認証子の有効性持続時間に基づいて計算され、前記有効性持続時間が、手動で設定される、または前記リモート配送システムにおいて動作するプログラムによって定義される、請求項1から3のいずれか一項に記載の方法。

30

【請求項5】

前記認証子に含まれる認証子識別情報(316)がブラックリスト(256)に記憶された別の認証子の識別情報と一致するかどうかをチェックすることによって、前記要求を検証するステップと、

一致する場合、前記要求は許可されず、結果として、前記ロックモジュールと前記少なくとも1つのモバイルデバイスとの間の切断となり、

前記ロックモジュールにより、前記少なくとも1つのモバイルデバイスからの切断要求に続いて、前記認証子識別情報および有効期限を前記ブラックリストに記憶し、関連付けるステップと、

40

前記ロックモジュールにより、前記少なくとも1つのモバイルデバイスと前記ロックモジュールとの間の短距離ワイヤレス通信の意図しない切断に続いて切断タイムアウト(258)に達した後、前記認証子識別情報および前記認証子の有効期限(314)を前記ブラックリストに記憶し、関連付けるステップと、

前記有効期限に達したとき、前記ブラックリスト内の前記認証子識別情報および前記有効期限を削除するステップと、

前記少なくとも1つのモバイルデバイスと前記ロックモジュールとの間の確立された短距離通信セッション内のすべての要求のために前記認証子を再利用するステップと、

前記少なくとも1つのモバイルデバイスが切断を要求するとき、前記ロックモジュールにより、前記認証子識別情報および前記有効期限を前記ブラックリストに記憶するステッ

50

ブと、

意図しない切断の場合、前記切断タイムアウトに達する前に、前記ロックモジュールとの接続を再確立するために前記認証子を再利用するステップと、

をさらに含む請求項1から4のいずれか一項に記載の方法。

【請求項6】

前記少なくとも1つの小荷物ロッカーのユーザの資格証明書に基づいて前記リモート配送システムによって生成された特権マスク(312)を前記認証子に含めるステップと、

前記ユーザに許可されている機能を定義する前記特権マスクに基づいて前記要求を検証するステップと、

機能テーブル(260)内の前記要求の対象となる機能を識別するステップと、

前記機能が前記特権マスクによって許可されているかどうかをチェックするステップと、

をさらに含む請求項1から5のいずれか一項に記載の方法。

【請求項7】

認証子識別情報は一意であり、一意にランダムに生成された文字列、または増分番号、または前記リモート配送システムによる認証子の生成の時間に対応する、請求項5または6に記載の方法。

【請求項8】

前記少なくとも1つのモバイルデバイスが、前記リモート配送システムと前記少なくとも1つの小荷物ロッカーの前記少なくとも1つの自律区画クラスタとの間の非同期双方向マルチチャネル通信を確立するためのモバイルデバイスのネットワークの一部として使用され、モバイルデバイスとの通信セッションがロックモジュールによって許可されると、他のモバイルデバイスからの要求が拒否され、前記少なくとも1つのモバイルデバイスが、前記少なくとも1つの小荷物ロッカーの前記少なくとも1つの区画を操作するためのユーザインターフェースとして使用され、前記少なくとも1つの小荷物ロッカーを操作するために前記少なくとも1つのモバイルデバイスにインストールされたプログラムが、前記少なくとも1つの小荷物ロッカーのユーザのログインに基づいて確立されたユーザカテゴリーに従ってインスタンス化される、請求項1から7のいずれか一項に記載の方法。

【請求項9】

第1の一意のクラスタ識別情報(250)を含む第1の前記ブロードキャストされたショートメッセージを捕捉した後、前記少なくとも1つの自律区画クラスタとの通信を確立するために、前記リモート配送システムにより、前記認証子を前記少なくとも1つのモバイルデバイスに要求するステップと、

前記リモート配送システムにより、前記少なくとも1つのモバイルデバイスから受信された前記第1の一意のクラスタ識別情報(250)に基づいて、前記少なくとも1つの小荷物ロッカーを識別するステップと、

前記リモート配送システムにより、前記認証子を生成し、または、第2の一意のクラスタ識別情報(134i)とともに前記認証子を送信するステップであって、前記認証子が区画インデックスを含み、区画インデックスが前記少なくとも1つの区画に関連付けられる、ステップと、

通信を確立するために、またはアクセスを許可するために、前記少なくとも1つのモバイルデバイスから受信された前記認証子を検証し、前記第2の一意のクラスタ識別情報を前記ロックモジュールに記憶された前記第1の一意のクラスタ識別情報(250)と比較するステップと、

をさらに含む請求項1から8のいずれか一項に記載の方法。

【請求項10】

前記少なくとも1つのモバイルデバイスを介して初期セットアップを実行するステップを含み、

前記少なくとも1つのモバイルデバイスにより、前記ロックモジュールから前記リモート配送システムへの前記シークレットキーの送信を安全にするために、前記リモート配送システムに公開鍵(152)を要求するステップと、

前記リモート配送システムにより、前記公開鍵および対応する秘密鍵(154)を生成するステップと、

前記公開鍵および前記秘密鍵をデータベース(130)に記憶し、関連付けるステップと、
前記リモート配送システムにより、前記公開鍵を前記少なくとも1つのモバイルデバイスに送信するステップと、

前記公開鍵を前記少なくとも1つのモバイルデバイスに一時的に記憶するステップと、
前記少なくとも1つのモバイルデバイスにより、前記ロックモジュールからブロードキャストされたショートメッセージを受信し、短距離ワイヤレス通信を確立するステップと、
前記少なくとも1つのモバイルデバイスにより、前記シークレットキーの生成を要求し、前記ロックモジュールに前記公開鍵を転送するステップであって、前記シークレットキーの生成の要求および前記公開鍵の転送が同じ要求内に含まれる、ステップと、

前記ロックモジュールにより、前記シークレットキーを生成するステップであって、前記シークレットキーがランダムに生成され、類似の場合に、前記リモート配送システムからの命令によって他のロックモジュールによって生成された他のシークレットキーと置き換えられる、ステップと、

前記シークレットキーを前記ロックモジュールに、暗号化された形式で記憶するステップと、

前記公開鍵で前記シークレットキーを暗号化するステップと、

前記シークレットキーを前記少なくとも1つのモバイルデバイスに暗号化された形式で送信するステップと、

前記少なくとも1つのモバイルデバイスにより、前記シークレットキーを、暗号化された形式で前記リモート配送システムに送信するステップと、

前記リモート配送システムにより、前記秘密鍵で前記シークレットキーを解読するステップと、

前記シークレットキーを、前記リモート配送システムの前記データベースに、クラスタシークレットキー(136i)として、暗号化された形式で、記憶するステップと、

前記シークレットキーを前記データベース内の前記ロックモジュールに一意に関連付けるステップと、

を含む、請求項1から9のいずれか一項に記載の方法。

【請求項11】

小荷物が前記少なくとも1つの区画内の預け入れの期日であるとき、前記少なくとも1つのモバイルデバイスにより、前記リモート配送システムによって生成される認証コード(270n)を前記リモート配送システムから受信し、モバイルデバイスのない小荷物の受取人がロックインターフェース(230)を介して前記認証コードを入力することによって前記小荷物を受け取ることができるように、前記認証コードを前記少なくとも1つの自律区画クラスタに転送するステップであって、前記認証コードが一意であり、前記小荷物の一意の小荷物識別情報(144j)に一意に関連付けられており、前記認証コードが、小荷物の受取人によって1回のみ使用することができるワンタイムコードである、ステップと、

預け入れのための前記小荷物が識別された後、前記少なくとも1つのモバイルデバイスにより、前記小荷物の預け入れ時に前記認証コードを要求するステップと、

前記認証コードを生成するステップと、

運送業者が前記少なくとも1つの小荷物ロッカーへの毎日の配達を計画する前または計画するときに、一時的な保管のために、前記リモート配送システムにより、前記認証コードを前記少なくとも1つのモバイルデバイスに伝達するステップと、

をさらに含む請求項1から10のいずれか一項に記載の方法。

【請求項12】

小荷物の預け入れおよび受け取りのための電子ロッカーシステムであって、
リモート配送システム(106)と、

長距離通信ネットワーク(104)を介して前記リモート配送システムと通信する少なくとも1つのモバイルデバイス(102)と、

10

20

30

40

50

ドア(116j)を備えた少なくとも1つの区画(112j)を含むとともにロックモジュール(120i)を含む少なくとも1つの自律区画クラスタ(110i)で構成される少なくとも1つの小荷物ロッカー(100)であって、前記ロックモジュール(120i)が、前記ドアのロックおよびロック解除を電子的に制御し、短距離通信(122i)を介して前記少なくとも1つのモバイルデバイスとローカルに通信する、前記少なくとも1つの小荷物ロッカー(100)と、

を備え、前記ロックモジュールが、

エネルギーモードの移行を管理し、前記少なくとも1つの自律区画クラスタをスリープモードで動作させることを可能にするように構成されたエネルギー管理モジュール(230)と、

アンテナ(218)を備えた無線トランシーバモジュール(216)と、

前記スリープモード中に、前記少なくとも1つのモバイルデバイス(102)との短距離通信セッションを確立するために、前記少なくとも1つのモバイルデバイスに向けて、ブロードキャストされたショートメッセージを前記無線トランシーバモジュール(216)で定期的に発するように構成された少なくとも1つのプロセッサ(210; 210A、210B、210C)と、

前記リモート配送システムによって生成され、暗号化され、前記少なくとも1つのモバイルデバイスによって送信された要求に含まれた認証子(300)を、不揮発性メモリ(240)に記憶されたシークレットキー(254)で解読するように構成された暗号化モジュール(256)と、

を含み、前記スリープモード中に、前記ロックモジュール(120i)は、ショートメッセージをブロードキャストするために部分的に起動され、前記無線トランシーバモジュール(216)は、アクティブ化され、前記エネルギー管理モジュール(230)によって制御され、前記認証子が、区画インデックス(310)、前記ロックモジュールに関するユーザ権利を定義する特権マスク(312)、有効期限(314)、および一意の認証子識別情報(316)を含むことを特徴とする、電子ロッカーシステム。

【請求項13】

前記ロックモジュールが、一意または実質的に一意の形式で、前記暗号化モジュールで前記シークレットキーを生成し、前記シークレットキーを前記不揮発性メモリに記憶するように構成され、前記ロックモジュールが、前記認証子の解読に基づく前記要求の自動検証のために構成され、認証コードは生成されず、前記自動検証のために前記ロックモジュールに提供されず、前記認証コードが、小荷物の受取人によって1回のみ使用することができるワンタイムコードであることを特徴とする、請求項12に記載のシステム。

【請求項14】

前記ロックモジュールが、前記少なくとも1つの自律区画クラスタに利用可能であるとともに前記少なくとも1つのプロセッサによって動作させることができる機能を含む機能テーブル(260)を前記不揮発性メモリに含み、前記認証子が、前記機能テーブル内の機能の中で前記少なくとも1つの自律区画クラスタを操作するために許可された機能を識別する特権マスク(312)を含み、前記特権マスクが、一連のビットで構成され、前記一連のビットのうちの1ビットが、前記機能テーブルのうちの1つの機能に対応し、前記ビットの値が、前記機能が許可されているか、あるいは許可されていないかを示し、前記リモート配送システムが、前記少なくとも1つの小荷物ロッカーのユーザの資格証明書を受信し、記憶し、前記認証子を生成し、前記資格証明書に基づいて前記特権マスクを生成するように構成されることを特徴とする、請求項12または13に記載のシステム。

【請求項15】

前記認証子が、前記認証子の有効性持続時間を制限する有効期限(314)、および前記リモート配送システムによって生成された認証子識別情報(316)を含み、前記ロックモジュールが、前記少なくとも1つのモバイルデバイスからの切断要求が発生したとき、または前記少なくとも1つのモバイルデバイスと前記ロックモジュールとの間の短距離ワイヤレス通信の意図しない切断に続いて切断タイムアウト(258)に達したとき、前記不揮発性メモリに、前記認証子識別情報と一致する有効期限に関連付けられた認証子識別情報、および前記認証子の前記有効期限を含むブラックリスト(256)を含むことを特徴とする、請求

10

20

30

40

50

項14に記載のシステム。

【請求項16】

前記ロックモジュールが、前記要求が検証されたとき、前記認証子識別情報と一致する有効期限に関連付けられた認証子識別情報、および前記認証子の前記有効期限を含むブラックリスト(256)を前記不揮発性メモリ内に含めることを特徴とする、請求項15に記載のシステム。

【請求項17】

前記暗号化モジュールが、前記シークレットキーを公開鍵(152)で暗号化し、前記少なくとも1つのモバイルデバイスを介して前記リモート配送システムに転送するためにデータを前記シークレットキーで暗号化するように構成され、前記シークレットキーを生成し、管理するための対称高度暗号化規格(AES)アルゴリズムを備えており、前記公開鍵でメッセージを解読するためのRSA2018非対称暗号化アルゴリズムまたは楕円曲線デジタル署名アルゴリズム(ECDSA)を備えており、前記リモート配送システムが、前記ロックモジュールに関連付けられるとともに前記シークレットキーに一致するクラスタシークレットキー(136i)をデータベース(130)に含み、リモート暗号化モジュール(156)を含み、前記公開鍵および関連する秘密鍵(154)が前記リモート暗号化モジュールによって生成されることを特徴とする、請求項12から16のいずれか一項に記載のシステム。

【請求項18】

前記ブロードキャストされたショートメッセージが、前記少なくとも1つの自律区画クラスタに関連する第1の一意のクラスタ識別情報(250)を含み、前記短距離通信を介して前記ロックモジュールとのローカル通信を確立するために前記少なくとも1つのモバイルデバイスからの要求が、第2の一意のクラスタ識別情報(134i)を含むまたは第2の一意のクラスタ識別情報(134i)とともに送信される前記認証子を含み、前記少なくとも1つのプロセッサが、前記ロックモジュールに記憶された前記第1の一意のクラスタ識別情報と前記第2の一意のクラスタ識別情報との間の一致をチェックするように構成されることを特徴とする、請求項17に記載のシステム。

【請求項19】

ロックインターフェース(226)を介して認証コードを入力することによって、モバイルデバイスのない小荷物の受取人が小荷物を受け取ることができるように、前記ロックモジュールが、前記ロックインターフェース(226)と、前記少なくとも1つの区画に預けられた小荷物に対応する一意の小荷物識別情報(144j)に一意に関連付けられた認証コード(270n)とを含み、前記リモート配送システムが、前記認証コードを生成し、記憶し、前記少なくとも1つのモバイルデバイスを介して前記ロックモジュールに前記認証コードを送信するように構成されることを特徴とする、請求項12から18のいずれか一項に記載のシステム。

【請求項20】

前記少なくとも1つのモバイルデバイスが、前記少なくとも1つの小荷物ロッカーの隣に、または前記少なくとも1つの小荷物ロッカーに直接に、固定して取り付けられ、ローカル電気ネットワークに接続されること、および前記少なくとも1つのプロセッサが、高エネルギープロセッサモジュール(210A)、低エネルギープロセッサモジュール(210B)、および超低エネルギープロセッサモジュール(210C)を含むことを特徴とする、請求項12から19のいずれか一項に記載のシステム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、配達業者によって荷物をロック可能な区画で構成された電子小荷物ロッカーに安全に預け、その後、これらの荷物を安全に受け取るためのシステムおよび方法に関する。

【背景技術】

【0002】

電子小荷物ロッカーシステムは、小荷物や小包など様々な種類の荷物を置いていき、保

10

20

30

40

50

管し、受け取るために使用される。これらの小荷物ロッカーシステムは、一般的に、荷物を預けるために運送業者によって使用され、荷物は、次いで、受取人によって、小荷物ロッカーから受け取られる。電子小荷物ロッカーには、運送業者の場合は荷物の預け入れ、受取人の場合は荷物の受け取りに使用される小荷物ロッカーを、運送業者または受取人が操作するためのユーザインターフェースがある。このインターフェースによって、ユーザは、小荷物ロッカーを操作するための情報を入力することができ、小荷物ロッカーは、ユーザに情報を返すことができる。最近の電子小荷物ロッカーでは、この機能は、一般的に、タッチスクリーンによって実現される。このユーザインターフェースは、荷物または何らかのユーザ識別手段に取り付けられた情報を捕捉するためにも使用される。この機能は、印刷されたバーコードを読み取るバーコードリーダー、またはRFIDタグを読み取るための無線周波数通信や短距離場通信など他の技術によって実現することができる。電子小荷物ロッカーシステムは、一般に、小荷物ロッカーのネットワークを備え、すべてが小荷物ロッカーのネットワークの管理を担当するリモート配送システムと直接通信し、最終的に運送業者情報システムとのデータ交換も管理する。各小荷物ロッカーとリモート配送システムとの間の通信は、GSMや3G/4Gなどの長距離通信技術によって実行される。

【0003】

図6は、長距離通信ネットワーク20を介してリモート配送システム25と通信する電子小荷物ロッカー10を含む先行技術の電子小荷物ロッカーシステムについて説明しており、リモート配送システム25は、電子小荷物ロッカーにアクセスするための認証コードを生成し、これらのコードを電子小荷物ロッカーに直接伝達し、電子小荷物ロッカーによって処理された荷物に関するデータを管理する。電子小荷物ロッカーは、電子制御ドアを備えた、異なるサイズの一連の区画30iを備える。電子小荷物ロッカーの操作、および特に区画ドアの開閉は、中央制御ユニット32によって制御される。この中央制御ユニット32は、リモート配送システム25と、典型的にはタッチスクリーン34およびバーコードリーダー36を含む小荷物ロッカーユーザインターフェースとの通信を制御する。小荷物を電子小荷物ロッカー10に預けるために運送業者が来ると、各小荷物40の識別情報38は、電子小荷物ロッカーによって捕捉されなければならない、中央制御ユニットによって、小荷物が預けられる区画と関連付けられる。追跡のために、識別情報38は、各小荷物40に添付されたバーコードラベルの形式であってもよい。一般に、区画は、標準の幅を有し、列42に垂直方向に組み立てられる。

【0004】

そのような先行技術の電子小荷物ロッカーシステムに関する第1の問題は、一般的に、電子小荷物ロッカーの使用を許可するコードが、小荷物ロッカーのユーザによって手動で入力されることである。電子小荷物ロッカーの使いやすさは、複雑すぎるコードの影響を受けることがないので、認証コードの複雑さは制限され、したがって、小荷物ロッカーアクセスのセキュリティが制限される。

【0005】

より一般的には、先行技術の電子小荷物ロッカーシステムとそれに関連するアーキテクチャにはいくつかの問題がある。電力接続が必要であり、これはしばしばセットアップが難しい場合がある。電子小荷物ロッカーとリモート配送システムのサーバとの間の長距離通信の必要性は、電子小荷物ロッカーを長距離通信ネットワークに接続する物理的な通信ケーブルの設置を強いる、またはワイヤレス長距離通信システムの使用を強いる。別の問題は、製造工場で組み立てられ、設置場所に完全なユニットとして出荷される先行技術の電子小荷物ロッカーに伴う複雑さおよびコストである。区画の垂直列は、一般的に、製造工場で事前に組み立てられ、部分的に事前に配線されている。そのようなアーキテクチャでは、区画を簡単に交換したり、現場で小荷物ロッカーの構成を簡単にアップグレードまたは変更したりすることができない。

【0006】

そのため、特に、区画の交換、およびセキュリティの向上を確実にすることを含め、コスト削減および柔軟性の向上を可能にする新世代の小荷物ロッカーが必要である。

【発明の概要】

【発明が解決しようとする課題】

【0007】

本発明の目的は、いくつかの自律区画クラスタを備えた小荷物ロッカーシステムを提供し、したがって、上記の欠点を克服することにある。

【課題を解決するための手段】

【0008】

この目的は、少なくとも1つの区画を含むとともにロックモジュールを含む少なくとも1つの自律区画クラスタで構成される少なくとも1つの小荷物ロッカーを、長距離通信ネットワークを介してリモート配送システムと通信する少なくとも1つのモバイルデバイスを介して操作するための方法を提供することによって達成され、この方法は、少なくとも1つのモバイルデバイスとリモート配送システムとの間の通信を確立するステップと、スリープモード中に、少なくとも1つのモバイルデバイスとの短距離通信セッションを確立するために、少なくとも1つのモバイルデバイスに宛てられたブロードキャストされたショートメッセージをロックモジュールによって定期的に発するステップと、少なくとも1つのモバイルデバイスによって、リモート配送システムから、前記リモート配送システムによって生成され、前記少なくとも1つのモバイルデバイスに暗号化された形式で提供された認証子を受信するステップであって、この認証子は、少なくとも1つのモバイルデバイスによって、認証子を含む要求をロックモジュールに送信するために使用される、ステップと、ロックモジュールに記憶されたシークレットキーにより、要求の自動検証のために認証子を解読するステップであって、認証コードは生成されず、要求の自動検証のためにロックモジュールに提供されない、ステップとを含む。有利には、認証子は一意である、または実質的に一意である。ショートメッセージのブロードキャストの結果として、区画クラスタに近接する任意の許可されていないモバイルデバイスは、ブロードキャストされたショートメッセージを受信し、通信の確立および区画へのアクセスを試みる場合がある。各要求への認証子の挿入に基づく本発明の許可方法は、許可されたモバイルデバイスと区画クラスタとの接続を確保し、また、ロックモジュールは、ロックモジュールに宛てられた各要求が提供されるので、認証子を記憶する必要がなくなる。

【0009】

好ましい実施形態では、認証子は、リモート配送システムによって生成され、ロックモジュールに関連付けられ、シークレットキーに一致するクラスタシークレットキーで暗号化される。好ましくは、クラスタシークレットキーは一意であり、ロックモジュールに一意に関連付けられている。

【0010】

本発明の特徴によれば、自動検証は、認証子に添付された署名を、解読後に認証子に基づいてロックモジュールにインストールされた暗号アルゴリズムによって計算された署名と比較することによって実行される。有利には、署名はハッシュである。本発明の別の特徴によれば、自動検証は、解読に続いて認証子の形式および内容を検証することによって実行され、または認証子に含まれる暗号ソルトを識別することによって、自動検証が実行される。したがって、モバイルデバイスを介した通信のセキュリティ、および区画へのアクセスは、上記の検証によって改善される。

【0011】

特定の実施形態では、要求は、認証子の有効期限に達したかどうかをチェックすることによってさらに検証され、有効期限に達した場合、要求は許可されず、結果として、ロックモジュールとモバイルデバイスとの間の切断となる。有利には、有効期限は、少なくとも1つの小荷物ロッカーのユーザカテゴリーに依存する認証子の有効性持続時間に基づいて計算され、したがって、有効期限は、セキュリティ上の理由で認証子の有効性持続時間を制限する。好ましくは、有効性持続時間は、手動で設定される、またはリモート配送システムにおいて動作するプログラムによって定義され、認証子の有効性持続時間は、一般的に、認証子が生成されてから使用され得るまでの持続時間に対応する。

【0012】

別の実施形態では、認証子に含まれる認証子識別情報がブラックリストに記憶されている別の認証子の識別情報と一致するかどうかをチェックすることによって、要求がさらに検証され、一致する場合、要求は許可されず、結果として、ロックモジュールとモバイルデバイスとの間の切断となる。ブラックリストは、認証子のいかなる無許可の再利用も防ぐために認証子の使用を一度だけ許可し、特に、次いで、ロックモジュールとの許可されていない通信を確立するために認証子を再利用する可能性がある許可されていない人によって認証子が捕捉されるリスクを防ぐことができる。

【0013】

本発明の特徴によれば、要求が許可されると、ロックモジュールは、認証子識別情報および認証子の有効期限をブラックリストに記憶し、関連付ける。有利には、ロックモジュールは、モバイルデバイスからの切断要求に続いて、認証子識別情報および有効期限をブラックリストに記憶し、関連付ける。

10

【0014】

本発明の別の特徴によれば、ロックモジュールは、少なくとも1つのモバイルデバイスとロックモジュールとの間の短距離ワイヤレス通信の意図しない切断に続いて切断タイムアウトに達した後、認証子識別情報および認証子の有効期限をブラックリストに記憶し、関連付け、したがって、生成される認証子の数が最小限に抑えられる。

【0015】

特定の実施形態では、有効期限に達し、ブラックリストにおいて認証子識別情報および有効期限が削除され、したがって、ロックモジュールにおけるデータストレージが最小限に抑えられる。

20

【0016】

好ましい実施形態では、少なくとも1つのモバイルデバイスとロックモジュールとの間の確立された短距離通信セッション内のすべての要求のために認証子が再利用され、したがって、通信セッション内のすべての要求に使用される生成された認証子の数が1つに最小化される。

【0017】

別の実施形態では、少なくとも1つのモバイルデバイスが切断を要求するとき、認証子識別情報および有効期限はロックモジュールによってブラックリストに記憶される。好ましくは、意図しない切断の場合、切断タイムアウトに達する前に、少なくとも1つのモバイルデバイスは、ロックモジュールとの接続を再確立するために認証子を再利用し、したがって、生成される認証子の数が最小限に抑えられる。

30

【0018】

本発明の特徴によれば、一意の認証子は、ユーザの資格証明書に基づいてリモート配送システムによって生成された特権マスクを含み、少なくとも1つの自律区画クラスタは、ユーザに許可されている機能へのアクセスを検証するために権限マスクを使用し、好ましくは、少なくとも1つの自律区画クラスタは、ロックモジュールを比較し、機能テーブル内の要求の対象となる機能を識別し、機能が特権マスクによって許可されているかどうかをチェックする。

40

【0019】

特定の実施形態では、認証子識別情報は一意であり、一意にランダムに生成された文字列、増分番号、またはリモート配送システムによる認証子の生成の時間に対応する。

【0020】

本発明の別の特徴によれば、少なくとも1つのモバイルデバイスは、リモート配送システムと少なくとも1つの小荷物ロッカーの少なくとも1つの自律区画クラスタとの間の非同期双方向マルチチャネル通信を確立するためのモバイルデバイスのネットワークの一部として使用され、したがって、認証子の使用による本発明の強固なセキュリティプロセスが必要である。

【0021】

50

好ましい実施形態では、モバイルデバイスとの通信セッションがロックモジュールによって許可されると、他のモバイルデバイスからの要求が拒否される。

【0022】

好ましくは、少なくとも1つのモバイルデバイスは、少なくとも1つの小荷物ロッカーの少なくとも1つの区画を操作するためのユーザインターフェースとして使用され、有利には、少なくとも1つの小荷物ロッカーを操作するために少なくとも1つのモバイルデバイスにインストールされたプログラムは、少なくとも1つの小荷物ロッカーのユーザのログインに基づいて確立されたユーザカテゴリーに従ってインスタンス化される。

【0023】

別の実施形態では、方法は、第1の一意のクラスタ識別情報を含む第1のブロードキャストされたショートメッセージを捕捉した後、少なくとも1つの自律区画クラスタとの通信を確立するために、認証子をリモート配送システムによって少なくとも1つのモバイルデバイスに要求するステップと、少なくとも1つのモバイルデバイスから受信された第1の一意のクラスタ識別情報に基づいて、少なくとも1つの小荷物ロッカーをリモート配送システムによって識別するステップとをさらに含む。

【0024】

本発明の特徴によれば、認証子は、リモート配送システムによって生成され、第2の一意のクラスタ識別情報を含むか、またはそれとともに送信され、区画インデックスを含み、ファームウェアは、区画インデックスを少なくとも1つの区画に関連付けるように構成される。

【0025】

特定の実施形態では、通信を確立するため、またはアクセスを許可するために、少なくとも1つの自律区画クラスタは、少なくとも1つのモバイルデバイスから受信された認証子を検証し、第2の一意のクラスタ識別情報をロックモジュールに記憶された第1の一意のクラスタ識別情報と比較する。

【0026】

好ましい実施形態では、ロックモジュールによってシークレットキーを生成し、ロックモジュールにシークレットキーを記憶するために、少なくとも1つのモバイルデバイスを介して初期セットアップが実行され、好ましくは、シークレットキーは、暗号化された形式で記憶される。したがって、セットアップは、どこでも行うことができる。

【0027】

別の実施形態では、シークレットキーはランダムに生成され、類似の場合に、リモート配送システムからの命令によって他のロックモジュールによって生成された他のシークレットキーと置き換えられる。

【0028】

本発明の別の特徴によれば、少なくとも1つのモバイルデバイスは、ロックモジュールからリモート配送システムへのシークレットキーの送信を安全にするために、リモート配送システムに公開鍵を要求する。

【0029】

好ましくは、リモート配送システムは、公開鍵および対応する秘密鍵を生成し、公開鍵および秘密鍵をデータベースに記憶し、関連付け、秘密鍵および公開鍵は、鍵の機密性の高い安全な転送を保証する。

【0030】

本発明の特徴によれば、公開鍵は、リモート配送システムによって少なくとも1つのモバイルデバイスに送信され、モバイルデバイスに一時的に記憶される。

【0031】

本発明の別の特徴によれば、少なくとも1つのモバイルデバイスは、ロックモジュールからブロードキャストされたショートメッセージを受信し、短距離ワイヤレス通信が確立され、少なくとも1つのモバイルデバイスは、シークレットキーの生成を要求し、ロックモジュールに公開鍵を転送する。

10

20

30

40

50

【0032】

好ましい実施形態では、交換の回数を最小限に抑えるために、また、公開鍵が送信されたかどうかに関するチェックが行われる必要がないように、シークレットキーの生成の要求および公開鍵の転送が同じ要求内に含まれる。好ましくは、ロックモジュールは、シークレットキーを公開鍵で暗号化し、シークレットキーを暗号化された形式でモバイルデバイスに送信する。

【0033】

特定の実施形態では、ロックモジュールに送信されるべきデータの暗号化、特に、認証子の暗号化、およびロックモジュールから受信されたデータの解読にシークレットキーを後で使うことができるように、シークレットキーは、少なくとも1つのモバイルデバイスによって暗号化された形式でリモート配送システムに送信され、秘密鍵によりリモート配送システムによって解読され、クラスタシークレットキーとしてリモート配送システムに記憶され、データベース内のロックモジュールに一意に関連付けられる。有利には、クラスタシークレットキーは、暗号化された形式でリモート配送システムに記憶される。

【0034】

特定の実施形態では、小荷物が少なくとも1つの区画に預けられる期日であるとき、少なくとも1つのモバイルデバイスは、リモート配送システムによって生成される認証コードをリモート配送システムから受信し、モバイルデバイスのない小荷物の受取人がロックインターフェースを介して認証コードを入力することによって小荷物を受け取ることができるように、認証コードを、少なくとも1つの自律区画に転送し、好ましくは、認証コードは一意であり、小荷物の一意の小荷物識別情報に一意に関連付けられており、有利には、認証コードは、小荷物の受取人によって1回のみ使用することができるワンタイムコードである。

【0035】

本発明の特徴によれば、認証コードは、預け入れのための小荷物が識別された後、小荷物の預け入れ時に少なくとも1つのモバイルデバイスによって要求される。

【0036】

本発明の別の特徴によれば、認証コードは、運送業者が少なくとも1つの小荷物ロッカーへの毎日の配達を計画する前または計画するときに、一時的な保管のために、リモート配送システムによって生成され、少なくとも1つのモバイルデバイスに伝達される。

【0037】

本発明はまた、小荷物の預け入れおよび受け取りのための電子ロッカーシステムに関し、システムは、リモート配送システムと、長距離通信ネットワークを介してリモート配送システムと通信する少なくとも1つのモバイルデバイスと、ドアを備えた少なくとも1つの区画を含み、ドアのロックおよびロック解除を電子的に制御し、短距離通信を介して少なくとも1つのモバイルデバイスとローカルに通信するロックモジュールを含む少なくとも1つの自律区画クラスタで構成される少なくとも1つの小荷物ロッカーとを備え、ロックモジュールが、エネルギーモードの移行を管理し、少なくとも1つの区画をスリープモードで動作させることを可能にするように構成されたエネルギー管理モジュールと、アンテナを備えた無線トランシーバモジュールと、スリープモード中に、少なくとも1つのモバイルデバイスに向けてブロードキャストされたショートメッセージを無線トランシーバモジュールで定期的に発するように構成された少なくとも1つのプロセッサと、リモート配送システムによって生成され、暗号化され、少なくとも1つのモバイルデバイスによって送信された要求に含まれた認証子を、不揮発性メモリに記憶されたシークレットキーで解読するように構成された暗号化モジュールと、を含む。

【0038】

本発明の別の特徴によれば、ロックモジュールは、暗号化モジュールでシークレットキーを生成し、シークレットキーを不揮発性メモリに記憶するように構成される。好ましくは、暗号化モジュールは、一意のシークレットキーまたは実質的に一意の鍵を生成するように構成される。

【0039】

特定の実施形態では、ロックモジュールは、認証子の解釈に基づく要求の自動検証のために構成され、認証コードは生成されず、自動検証のためにロックモジュールに提供されない。

【0040】

別の実施形態では、ロックモジュールは、少なくとも1つの自律区画クラスタに利用可能であり、少なくとも1つのプロセッサによって実行することができる機能を含む機能テーブルを記憶する不揮発性メモリを含み、有利には、一意の認証子は、機能テーブル内の機能の中で少なくとも1つの自律区画クラスタを操作するために許可された機能を識別する特権マスクを含み、好ましくは、特権マスクは、一連のビットで構成され、一連のビットのうちの1ビットは、機能テーブルのうちの1つの機能に対応し、ビットの値は、機能が許可されているかどうかを示す。

10

【0041】

本発明の特徴によれば、リモート配送システムは、少なくとも1つの小荷物ロッカーのユーザの資格証明書を受信し、記憶し、一意の認証子を生成し、ユーザの資格証明書に基づいて特権マスクを生成するように構成される。

【0042】

好ましい実施形態では、認証子は、認証子の有効性持続時間を制限する有効期限を含む。有利には、認証子は、リモート配送システムによって生成された認証子識別情報を含む。

【0043】

本発明の別の特徴によれば、要求が検証されると、ロックモジュールは、不揮発性メモリ内に、認証子識別情報と一致する有効期限に関連付けられた認証子識別情報、および認証子の有効期限を含むブラックリストを含む。

20

【0044】

好ましい実施形態では、暗号化モジュールは、シークレットキーを公開鍵で暗号化し、少なくとも1つのモバイルデバイスを介してリモート配送システムに転送するためのデータをシークレットキーで暗号化するように構成される。

【0045】

特定の実施形態では、暗号化モジュールは、シークレットキーを生成し、管理するための対称高度暗号化規格(AES)アルゴリズムを備え、メッセージを公開鍵で解読するためのRSA2018非対称暗号化アルゴリズムまたは楕円曲線デジタル署名アルゴリズム(ECDSA)を備える。

30

【0046】

別の実施形態では、リモート配送システムは、ロックモジュールに関連付けられ、シークレットキーと一致するクラスタシークレットキーをデータベースに含む。好ましくは、リモート配送システムは、リモート暗号化モジュールを含み、公開鍵および関連する秘密鍵はリモート暗号化モジュールによって生成される。公開鍵および秘密鍵が、ロックモジュールとリモート配送システムとの間で暗号化された形式でシークレットキーを転送するために使用される。

【0047】

本発明の特徴によれば、ブロードキャストされたショートメッセージは、少なくとも1つの自律区画クラスタに関連する第1の一意のクラスタ識別情報を含む。

40

【0048】

本発明の別の特徴によれば、短距離通信を介してロックモジュールとのローカル通信を確立するための少なくとも1つのモバイルデバイスからの要求は、第2の一意のクラスタ識別情報を含む、またはそれとともに送信される認証子を含み、少なくとも1つのプロセッサは、ロックモジュールに記憶されている第1の一意のクラスタ識別情報と第2の一意のクラスタ識別情報との一致をチェックするように構成される。

【0049】

特定の実施形態では、少なくとも1つの区画クラスタのいくつかが互いに機械的に固定

50

されて列を形成し、好ましくは、少なくとも1つの自律区画クラスタの列のいくつかが互いに機械的に固定されて少なくとも1つの小荷物ロッカーを形成し、したがって、区画クラスタの交換を含む、簡単な設置および構成のアップグレードおよびサービスが可能になる。

【0050】

別の実施形態では、認証子は、区画インデックスを備え、プロセッサは、区画インデックスを少なくとも1つの区画に関連付けるように構成される。

【0051】

好ましい実施形態では、ロックモジュールは、ロックインターフェースと、少なくとも1つの区画に預けられた小荷物に対応する一意の小荷物識別情報に一意に関連付けられた認証コードとを含み、したがって、ロックインターフェースを介して認証コードを入力することによって、モバイルデバイスのない小荷物の受取人が小荷物を受け取ることができるようにし、リモート配送システムは、認証コードを生成し、記憶し、モバイルデバイスを介してロックモジュールに認証コードを送信するように構成される。

【0052】

有利には、少なくとも1つのモバイルデバイスは、少なくとも1つの小荷物ロッカーの隣に、または少なくとも1つの小荷物ロッカーに直接固定して取り付けられ、ローカル電気ネットワークに接続されており、前記少なくとも1つのプロセッサは、高エネルギープロセッサモジュール、低エネルギープロセッサモジュール、および超低エネルギープロセッサモジュールを含むことができる。

【0053】

本発明の教示の他の態様、特徴、および利点は、添付の図面と併せて以下の説明を検討すると、当業者には明らかになるであろう。

【図面の簡単な説明】

【0054】

【図1】本発明の一実施形態による小荷物ロッカーシステムのアーキテクチャを表す図である。

【図2】本発明の一実施形態によるロックモジュールのアーキテクチャを示す図である。

【図3】本発明の認証子の一実施形態を示す図である。

【図4】ロックモジュールをセットアップするための本発明の一実施形態によるプロセスを示す図である。

【図5】ロックモジュールによってモバイルモジュールからの要求を検証するための本発明の一実施形態によるプロセスを示す図である。

【図6】先行技術の電子小荷物ロッカーシステムを示す図である。

【発明を実施するための形態】

【0055】

本発明によれば、電力接続および長距離通信の必要性を回避し、簡単な設置および構成のアップグレードを可能にするために、短距離ワイヤレス通信を介してモバイルデバイスとローカルに対話する区画の自律クラスタが開示される。図1は、小荷物ロッカー100と、3G-4GまたはGSMなどの技術に基づく長距離通信ネットワーク104を介して、小荷物ロッカー100への認証アクセスを管理し、小荷物ロッカー100によって処理される出荷に関するデータを管理するリモート配送システム106と通信するモバイルデバイス102とを備える本発明の小荷物ロッカーシステムの一実施形態を示す。小荷物ロッカー100は、いくつかの区画112jを備え得る自律区画クラスタ110iから構成される。同じ幅を有する区画112jおよび自律区画クラスタ110iは、異なる小荷物サイズとの最適な一致に対処するために異なる高さを有してもよい。そのような区画クラスタは、一般的に、2つまたは3つの区画を備え、または最終的には1つの大きい区画のみを備える。区画クラスタを積み上げて機械的に固定し、列114を形成することができる。次いで、列114を機械的に固定して、より大きい小荷物ロッカーユニットを形成することができる。自律区画クラスタは、いかなる電力接続または長距離通信もない設計によって特徴付けられ、簡単な設置および構成

のアップグレードが可能である。各区画112jには、正面にヒンジ付きドア116jが備えられており、このドア116jを開くと、区画に小荷物118jを預ける、または区画から小荷物118jを取り出すことができる。各自律区画クラスタ110iは、クラスタの区画の各ドアのロックおよびロック解除を電子的に制御する通信ロックモジュール120iを備える。各ロックモジュール120iは、WIFI、IR、またはBluetoothなどの短距離ワイヤレス通信122iを介して近くのモバイルデバイス102とのローカル通信を確立することができる。好ましくはスマートフォンまたはPDAなどのモバイルデバイスであるが、デバイス102は、ロックモジュールの短距離通信機能と互換性のあるいくつかの短距離ワイヤレス通信機能を有するPCまたはラップトップなどの固定のコンピュータ化されたデバイスであってもよい。

【0056】

モバイルデバイス102は、スマートフォンもしくは携帯情報端末(PDA)、またはロックモジュールの短距離通信機能と互換性のあるいくつかの短距離ワイヤレス通信機能を有し、リモート配送システム106の長距離通信機能と互換性のあるいくつかの長距離通信機能を有する任意のコンピュータ化されたモバイルデバイスとすることができる。本発明によれば、モバイルデバイスは、小荷物ロッカーの区画を操作するためのユーザインターフェースとして使用され、先行技術の小荷物ロッカーの中央ユーザインターフェースに取って代わり、したがって、本発明の小荷物ロッカーには必要ない。より一般的には、モバイルデバイスは、リモート配送システムと小荷物ロッカーのロックモジュールとの間の通信のためのチャンネルとして使用され、非同期双方向マルチチャンネル通信の確立を可能にする。結果として、リモート配送システムは、たとえば、区画の操作をブロックするための命令を任意のモバイルデバイスを介して転送する、または区画クラスタのロックモジュールは、リモート配送システムに対して、区画クラスタの区画内の操作に関するイベントなどの情報を、任意のモバイルデバイスを介して転送し得る。したがって、モバイルデバイスを介した通信を安全にすること、ならびにモバイルデバイスを介した区画へのアクセスが必須である。

【0057】

異なるカテゴリーのユーザは、一般的にPDAを使用し得る小荷物の受取人、サイト所有者、または運送業者を含むモバイルデバイスを介して小荷物ロッカーの区画と対話することができる。好ましくは、特に、小荷物の受取人の場合、モバイルデバイスはスマートフォンであり、したがって、小荷物の受取人は個人のスマートフォンを使用することができる。小荷物ロッカー区画をローカルで操作するためのモバイル小荷物ロッカーアプリケーション(MPLアプリケーション)がモバイルデバイスにインストールされてもよく、好ましくは、たとえばアプリケーションストアを介してリモートサーバからダウンロードされてもよい。小荷物ロッカーサービスへの最も簡単に広範なアクセスを提供するために、MPLアプリケーションは、Google PlayやApp Storeなどの標準的なアプリケーションストアからダウンロードされてもよい。MPLアプリケーションは、一般的にサイト所有者にとっては、小荷物ロッカーを設置し、またはサービスするための、または一般的に運送業者にとっては、小荷物を配達するための、または一般的に荷物の受取人にとっては、小荷物を受け取るため、または通知を受信するためのサブプログラムを含む。好ましくは、MPLアプリケーションは、ユーザカテゴリーに従ってインスタンス化される。運送業者のPDAの場合、MPLアプリケーションは、小荷物を配達するためにそのPDAにインストールされた運送業者ソフトウェアモジュールに統合されてもよい。MPLアプリケーションへのそのような簡単にオープンなアクセスは、モバイルデバイスを介した通信が安全にされ、モバイルデバイスを介した区画へのアクセスも必要とし、システムセキュリティは、以下で説明するように、本発明の認証機能およびプロセスによって対処される。

【0058】

許可されていないデバイスからの任意の通信および最終的に区画への任意のアクセスを防ぐために、通信セッションを確立するためのモバイルデバイスからの要求の一部として、認証子、好ましくは一意の認証子が提供される必要があり、この認証子は、通信セッションの確立を許可し、最終的にモバイルデバイスからの任意の要求を許可するために、区

画クラスタのロックモジュールによってチェックされる。認証子は、リモート配送システムによって、暗号化された形式で、許可されたモバイルデバイスに提供される。次いで、認証子は、通信セッションを確立するために、モバイルデバイスによってロックモジュールに提供され、認証子は、要求を検証するためにロックモジュールによって解読される。その結果、受取人が小荷物ロッカーの近くにいるときに小荷物ロッカーの区画にアクセスするために、小荷物の受取人のモバイルデバイスによって認証子が自動的に送信され得る。先行技術のように小荷物ロッカーのユーザインターフェースを介して認証コードを入力する必要がなく、したがって、アクセスセキュリティおよびユーザ体験が向上する。

【0059】

リモート配送システムはデータベースシステム130を備え、データベースシステム130は、運送業者によって、または小荷物ロッカーパークを所有または管理するサービス会社によって操作されるいくつかのサーバシステムに最終的にインストールされるいくつかのデータベースを含み得る。データベースシステム130は、リモート配送システムによって制御されるべきすべての小荷物ロッカー100の構成を記憶する。各小荷物ロッカー構成(PL構成)は、一意の小荷物ロッカー識別132を含み、小荷物ロッカーの区画クラスタ110iごとに、一意のクラスタ識別情報134iおよび好ましくは一意のクラスタシークレットキー136iを含む。PL構成は、区画クラスタごとに、ロックモジュールがモバイルデバイスに向けてショートメッセージをブロードキャストするための最適化されたパラメータに対応する、反復時間期間パラメータ、リスニング時間ウィンドウパラメータ、および電力放出パラメータを含むクラスタブロードキャストテーブル138iも含む。区画クラスタの各区画は、同じくデータベース130に記憶されている区画インデックスによって識別され、区画クラスタの区画の中の区画をインデックス付けする。一意のクラスタ識別情報および区画インデックスの関連付けによって、区画の一意の識別が可能になる(一意の区画識別)。さらに、PL構成は、区画112jごとに、ユーザの視覚的識別子として区画クラスタにおいて複製される区画識別子140j、区画サイズ142j、および区画112jに小荷物が預けられている場合、一意の小荷物識別情報144jを含む。データベースシステム130は、小荷物ロッカーのユーザの資格証明書、および電話番号や電子メールアドレスなど、小荷物ロッカーのユーザと通信するための情報も記憶する。特に、データベースシステム130は、小荷物の受取人ごとに、小荷物の受取人が小荷物を受け取るために必要であり得、区画に預けられた小荷物ごとにリモート配送システムによって生成される一意の認証コード150jを記憶する。一意の認証コード150jは、受取人の資格証明書に関連付けられ、対応する小荷物の小荷物識別情報144jに一意に関連付けられる。

【0060】

公開鍵152はデータベース130に記憶されており、ロックモジュールとリモート配送システムとの間でシークレットキーを転送するために使用される。公開鍵152に関連付けられた秘密鍵154もデータベースに記憶され、秘密鍵で暗号化されたデータを解読するために使用される。リモート配送システムは、関連する秘密鍵および公開鍵を生成し、特にシークレットキーを送信するために、秘密鍵でデータを解読し、たとえば、モバイルデバイスを介してロックモジュールにデータを転送するために、シークレットキーでデータを暗号化し、たとえば、モバイルデバイスを介してロックモジュールから受信されたデータなど、シークレットキーでデータを解読するように構成されたりリモート暗号化モジュール156を備える。リモート暗号化モジュールには、非対称暗号化アルゴリズム、好ましくは、公開鍵および秘密鍵を生成し、管理するための楕円曲線デジタル署名アルゴリズム(ECDSA)などの楕円曲線暗号(ECC)タイプのアルゴリズムまたはRSA2018アルゴリズムが備えられており、対称暗号化アルゴリズム、好ましくは、シークレットキーでメッセージを暗号化し、解読するための高度暗号化規格(AES)アルゴリズムが備えられている。

【0061】

自律区画クラスタの使用は、特に、区画クラスタの周囲の任意の電気配線または任意の電力接続の必要性を回避するので、簡単さおよび柔軟性を提供する。しかしながら、各区画クラスタの電力消費を最小限に抑える重要な要求があり、したがって、エネルギー消費

10

20

30

40

50

の重要な原因である通信およびデータ交換を最小限に抑えるためのロックモジュール、およびロックモジュール内のデータストレージが必要である。電力消費を最小限に抑える1つの方法は、ロックモジュールの動作のために低エネルギーモードまたはスリープモードを実装することである。並行して、特に、たとえば、長いデータ交換のために、ユーザが小荷物ロッカーの前で長時間待つ必要がないことを確実にすることを含めて、小荷物ロッカーの使いやすさを最適化する必要がある。これらの態様は、以下で詳述するように、本発明によって対処される。

【0062】

図2は、バス214または直接制御ラインを介してロックモジュールの主要コンポーネントを制御するプロセッサまたはプロセッサ210のグループおよび関連する揮発性メモリ212を備える区画クラスタ110iのロックモジュール120iを示す。短距離ワイヤレス通信は、アンテナ218を備えた無線トランシーバモジュール216によって実行される。無線トランシーバモジュールは、いくつかのレジスタを含んでいてもよく、またはロックモジュールメモリ内の専用レジスタにアクセスでき得る。無線トランシーバモジュールに専用のこれらのレジスタは、無線トランシーバモジュールおよびアンテナの動作のための設定データ、ならびにモバイルデバイスまたはいくつかのモバイルデバイスとの通信を開始するためのロックモジュールによって送信される初期メッセージまたはブロードキャストショートメッセージに関するデータを含む。区画クラスタの各区画のドアには、電気錠220nが備えられている。電気錠の戸締りは、特にプロセッサ210の制御下で電気錠に電力を供給し、プロセッサ210によって直接制御される電力段221を介して実行される。センサー222nは、電気錠の状況(ロック/ロック解除)またはドアの状況(開/閉)または区画が空か一杯かを確定するために、区画ごとに提供されてもよい。センサーの電力供給およびセンサーによって実行される測定は、ロックモジュールのセンサー入出力ポート(I/O)223を介して提供される。発光ダイオード(LED)などの視覚インジケータ224nは、たとえば、どの区画を小荷物の預け入れまたは受け取りに使用すべきかを示すために、各区画に取り付けられ、プロセッサによって制御され得る。インジケータへの電力供給は、ロックモジュールのインジケータ入出力ポート(I/O)225を介して提供される。好ましくは、ドアがロック解除されると、たとえばバネ機構のおかげで、ドアは、自動的に開き、したがって、いかなる視覚インジケータも必要とせずに、どの区画が使用されるべきかを示す。システムは、小荷物の受取人によってスマートフォンなどのモバイルデバイスにより操作されるように設計されているが、モバイルデバイスを所有していない小荷物の受取人が、ロックインターフェースで認証コードを入力することによって区画にアクセスすることができるよう、ピンパッドまたは当技術

分野で知られている別のインターフェースなどのロックインターフェース226も、その小荷物の受取人に提供される。ユーザが特定の区画を識別し得るように、番号などの区画識別子を各区画の可視部分、たとえばドアなどに取り付けてもよい。したがって、モバイルデバイスを所有していない受取人は、小荷物を受け取る必要のある区画、および区画の近くにある関連するロックインターフェースを識別し得る。代替的に、ユーザが特定の区画クラスタおよび関連するロックインターフェースを識別できるように、番号などのクラスタ識別子が各区画クラスタの可視部分に添付されてもよい。したがって、モバイルデバイスを所有していない受取人は、小荷物を受け取る必要がある区画クラスタを識別し、対応するロックインターフェースを使用して区画を開くようにしてもよい。

【0063】

ロックモジュールは、電源228によって電力供給され、電源228は、ソーラーパネルまたはエネルギー採取機器または任意の他の電気エネルギー供給を介した交換可能なバッテリーまたは充電式バッテリーであり得る。電力消費を最小限に抑えるために、エネルギー管理モジュール230は、エネルギーモードの移行を管理し、区画クラスタ110iを異なる低エネルギーモードまたは異なるスリープモードで動作させることを可能にする。各エネルギーモードは、利用可能な周辺機器またはコンポーネントを定義し、周辺機器またはコンポーネントによって消費される電流量を制限する。たとえば、エネルギー管理モジュール

10

20

30

40

50

は、揮発性メモリ212の未使用ブロックの電源をオフもしくはオンにする、または無線トランシーバモジュールをオフもしくはオンにしてもよい。エネルギー管理モジュールは、電圧調整器およびエネルギーモード間を切り替えるためのタイマーを備えてもよい。

【0064】

プロセッサによって制御され、直接アクセス可能な不揮発性メモリ240は、プロセッサ210によって実行されるファームウェア、および、動作イベントなど、モバイルデバイスを介してリモート配送システムから受信された、または区画クラスタ110i内で生成されたデータを記憶する。不揮発性メモリ240に記憶されたデータは、区画クラスタを一意に識別するクラスタ識別情報250、区画クラスタの区画の中の各区画のインデックス付けに使用される区画インデックス252n、シークレットキー254、モバイルデバイスとの通信確立を管理するためのブラックリスト256、およびモバイルデバイスとロックモジュールとの間の短距離ワイヤレス通信の意図しない切断を管理するための切断タイムアウト258を含む。不揮発性メモリ240は、区画クラスタ操作に利用可能であり、許可されたモバイルデバイスによる要求時にプロセッサ210によって実行することができるすべての機能に対応する機能テーブル260も記憶し、区画クラスタの区画ごとに、区画内の小荷物を受け取るために受取人から要求され得る一意の認証コード270nを記憶してもよく、クラスタブロードキャストテーブル272を記憶してもよい。

【0065】

また、ロックモジュールは、シークレットキー254を生成するため、たとえば、モバイルデバイスを介してリモート配送システムに転送するために、シークレットキーでデータを暗号化するため、たとえば、モバイルデバイスを介してリモート配送システムから受信されたデータについて、シークレットキーでデータを解読するため、および、特に、モバイルデバイスを介してリモート配送システムに転送するために、生成されたシークレットキーを暗号化するために、公開鍵152でデータを暗号化するように構成された暗号化モジュール256を備える。小荷物ロッカーのセットアップ段階中、各ロックモジュールは、好ましくは一意のシークレットキーを生成し、記憶し、シークレットキーは、次いで、リモート配送システムに送信され、各特定のロックモジュールおよびクラスタに一意に関連付けられたクラスタシークレットキー136iとしてリモート配送システムに記憶される。ロックモジュールまたはリモート配送システムのいずれかによる特定のシークレットキーによるデータの暗号化によって、モバイルデバイスを介した安全で機密性の高い交換が可能になる。暗号化モジュール256には、対称暗号化アルゴリズム、好ましくは、シークレットキーを生成し、管理するための高度暗号化規格(AES)アルゴリズムが備えられ、非対称暗号化アルゴリズム、好ましくは、公開鍵でメッセージを解読するための楕円曲線デジタル署名アルゴリズム(ECDSA)などの楕円曲線暗号(ECC)タイプのアルゴリズムまたはRSA2018アルゴリズムが備えられる。

【0066】

シークレットキー254は、他のロックモジュールによってランダムに生成された鍵との非常に低い確率の類似性で暗号化モジュール256によってランダムに生成され得、したがって実質的に一意である。たとえば、キーをランダムに生成するAES256暗号化モジュールの場合、類似の確率は、10の77乗に1つのチャンスよりも低い。そのような場合、リモート配送システムは、類似性をチェックし、シークレットキーの統一性を保証するようにいくつかのシークレットキーの変更を指示する。

【0067】

短距離ワイヤレス通信を介してロックモジュール120iと通信するために、モバイルデバイス102は、関連する短距離ワイヤレス通信ソフトウェアを実行するプロセッサによって制御されるアンテナを備えた無線トランシーバモジュールも備える。特に、モバイルデバイス102は、通信する必要がある異なる区画クラスタを発見するためのスキャン機能を備える。そのようなハードウェアおよびソフトウェアコンポーネントは、スマートフォンまたはPDAで一般的に利用可能である。

【0068】

区画クラスタが使用されていないとき、ロックモジュールはディープスリープモード、すなわち、区画クラスタの電力消費を最小限に抑えるために非常に低いエネルギーモードである。そのようなディープスリープモードでは、区画クラスタのエネルギーレベルは、区画クラスタが起動して完全に動作しているときの平均エネルギー消費量の10%未満である。非常に限られた機能しか利用できず、特に、無線トランシーバモジュールはスリープ状態であり、ロックモジュールは、区画クラスタの近くのモバイルデバイスと通信することができず、それによって起動することができない。ディープスリープモードのとき、モバイルデバイスとの通信セッションを開始できるようにするため、ロックモジュールは、ショートメッセージをブロードキャストするために一時的に部分的に起動する。低エネルギースリープモードに対応するこの部分的な起動は、無線トランシーバモジュールをアクティブにし、スリープモードへの移行をトリガするための低エネルギースリープタイマー280を備えることができるエネルギー管理モジュールによって制御することができる。スリープモードでは、追加の機能は、ディープスリープモードと比較して、ブロードキャストされたショートメッセージの送信および応答の待機に制限される。ロックモジュールの動作は、スリープモードで非アクティブ化される、通信管理およびアクセス許可管理を含む高レベルの機能を制御する高エネルギープロセッサモジュール210A、ディープスリープモードで非アクティブ化される、ブロードキャストされたショートメッセージを送信し、応答を待つための無線トランシーバモジュールを制御する低エネルギープロセッサモジュール210B、および最小限の制御のための非常に低いエネルギープロセッサモジュール210Cを備えるいくつかのプロセッサモジュールで構成されるプロセッサによって制御することができる。エネルギー管理モジュールは、これらのモードと関連するエネルギー消費との間の切り替えを管理する。ロックモジュールの動作は、一緒に連携し、そのアクティビティおよびエネルギー消費がエネルギー管理モジュールによって管理される別々のプロセッサによって制御することもできる。たとえば、特定のプロセッサは、無線トランシーバモジュールを制御してもよく、スリープモード中に特に起動されてもよい。

【0069】

電力消費を最小限に抑えるために、ロックモジュールは、一般に、ディープスリープモードに維持される。モバイルデバイスとの通信を可能にするために、低エネルギースリープタイマー280は、反復時間期間に従ってディープスリープモードからスリープモードへの移行を定期的にトリガする。ひとたびスリープモードになると、ロックモジュールは、ブロードキャストされたショートメッセージを送信し、制限されたリスニング時間ウィンドウの間にモバイルデバイスからの応答をアクティブにリスンする。リスニング時間ウィンドウの終了は、エネルギー管理モジュールに含めることができるリスニング時間ウィンドウタイマー282によってトリガされる。区画クラスタに近接し、短距離ワイヤレス通信がアクティブ化されたモバイルデバイスは、ロックモジュールからブロードキャストされたショートメッセージをリスンするスキャン機能を有する。モバイルデバイスは、ロックモジュールからブロードキャストされたショートメッセージを捕捉したとき、ロックモジュールとの通信を確立する必要がある場合、応答メッセージをロックモジュールの制限されたリスニング時間ウィンドウ内に捕捉できるように、通信を確立するために、応答メッセージをロックモジュールにすぐに送信する。

【0070】

モバイルデバイスからの応答メッセージの無線トランシーバモジュールによる受信は、ロックモジュールの完全な起動をトリガする。エネルギー管理230は、高レベル機能を制御する高エネルギープロセッサモジュール210Aをアクティブ化することによって、または互いに協働する別個のプロセッサを有するアーキテクチャの場合に対応するプロセッサをアクティブ化することによって、プロセッサ高レベル機能をアクティブ化する。モバイルデバイスとの通信を確立するために、スリープモードではロックモジュールがモバイルデバイスとの通信セッションの認証を実行することができず、通信の確立を完了することができないので、ロックモジュールの完全な起動が必要である。通信が確立されると、モバイルデバイスは、次いで、要求およびコマンドを開始し、ロックモジュールからの応答

を受け入れるクライアントとして挙動する。ロックモジュールは、要求およびコマンドを受信し、要求されたアクションを実行し、応答を返すサーバとして挙動する。その結果、区画クラスタに近接する任意の許可されていないモバイルデバイスは、区画クラスタからブロードキャストされたショートメッセージを受信し、通信の確立および区画へのアクセスを試みる場合がある。認証子の使用に基づく本発明の許可方法は、許可されたモバイルデバイスと区画クラスタとの接続を安全にする。

【0071】

ブロードキャストされたショートメッセージに対するモバイルデバイスからの応答が、制限されたリスニング時間ウィンドウ内に無線トランシーバモジュールによって捕捉されない場合、リスニング時間ウィンドウタイマー282は、スリープモードの終了をトリガし、エネルギー管理230は、ディープスリープモードへの戻りを管理し、無線トランシーバモジュールおよび低エネルギープロセッサモジュール210Bを非アクティブ化する。

【0072】

モバイルデバイスが特定の区画クラスタからブロードキャストされたショートメッセージを受信すると、モバイルデバイスは、たとえば、区画クラスタに記憶されたイベントをリモート配送システムに転送したり、区画クラスタの区画に小荷物を預けたり、区画クラスタの区画から小荷物を受け取ったりするために、その特定の区画クラスタとの通信セッションを確立する必要がある場合がある。任意の通信および最終的に許可されていないデバイスから区画クラスタへの任意のアクセスを防ぐために、通信セッションを確立するためのモバイルデバイスからの要求の一部として、リモート配送システムによって生成される好ましくは一意の認証子を提供する必要がある。

【0073】

認証子は、要求が適切な区画クラスタに宛てられることを確実にするために、ロックモジュールによってチェックされる一意のクラスタ識別情報を含むか、それとともに送信され、(たとえば、その特定の区画への預け入れ、またはその特定の区画からの受け取りのために)確立されている通信セッションに関連付けられた区画を識別する区画インデックスを含む。通信セッションを確立するためのモバイルデバイスからの要求は、他の区画クラスタによって受信される場合があるが、クラスタ識別情報において一致がないので拒否される。モバイルデバイスとの区画クラスタによる通信セッションが許可されると、他のモバイルデバイスからの要求が拒否される。通信セッション中、モバイルデバイスから区画クラスタへの任意の要求は、認証子を含む必要があり得る。認証子は、リモート配送システムによって生成され、リモート配送システムによってモバイルデバイスに提供される。

【0074】

図3は、本発明の認証子300の一実施形態を示す。ロックモジュール120iとモバイルデバイス102との間の交換の回数を最小限に抑えるために、認証子は、ロックモジュールが後でモバイルデバイスに要求する必要がないように、いくつかの重要なデータを含む。認証子は、確立されている通信セッションに関連付けられた区画を識別する区画インデックス310(たとえば、その特定の区画への預け入れまたはその特定の区画からの受け取り)、および機能テーブル260内の利用可能なすべての機能の中で、許可されている機能を識別する特権マスク312を含む。リモート配送システムによる特権マスクの生成は、ユーザ、特にユーザカテゴリーに依存する。次いで、リモート配送システムは、認証子内の特権マスクをモバイルデバイスに提供する。特権マスクおよび認証子は、ユーザがMPLアプリケーションにログインするとリモート配送システムによって生成され、MPLアプリケーションは、小荷物ロッカー区画と対話するためにモバイルデバイスにインストールされ、リモート配送システムに認証子を自動的に要求する。通信セッションの確立に続いて、区画クラスタが特定のユーザに許可されている機能へのアクセスを提供するために、区画クラスタによって受信された特権マスクが使用される。特権マスクは、揮発性メモリに記憶され、特定のユーザに許可された機能をチェックするためにロックモジュールによって実行されるファームウェアによって対処される。特権マスクのサイズを最小限に抑え、したがって、ロックモジュールと交換されるデータボリュームを最小限に抑えることに関与するた

10

20

30

40

50

めに、特権マスクは、好ましくは32ビットまたは64ビットシリーズの、一連のビットで構成され、各ビットは、機能テーブル260のうちの1つの特定の機能に対応する。ビット値は、機能が許可されているかどうかを示す。たとえば、1に設定されたビットは機能が許可されていることを示し、0に設定されたビットは機能が許可されていないことを示す場合がある。特権マスクのそのような形式によって、情報の圧縮および認証子への特権マスクの便利な組み込みが可能になり、これによって、許可された機能を定義するために、区画クラスタとモバイルデバイスとの間の追加の通信の必要性がなくなる。認証子はまた、その後は認証子がもはや有効ではない有効期限314も含む。有効期限は、セキュリティ上の理由から認証子の有効性持続時間を制限する。一般的に、認証子の有効性持続時間は、認証子が生成される時間と、たとえば、小荷物の受取人による受け取りまたは配達業者による小荷物の預け入れに使用され得る時間との間の持続時間に対応し、最高数日までとすることができる。有効期限は、有効性持続時間に基づいてリモート配送システムによって計算され、これは、ユーザカテゴリーまたは他の使用条件に依存し、リモート配送システムで構成され得る。小荷物の受取人の場合、有効性持続時間は、一部の区画スペースを解放するために運送業者が荷物を取り除く前に、小荷物を受け取るために受取人に与えられた時間に対応し、2日から5日の間でもよい。運送業者の場合、有効性持続時間は、運送業者が小荷物ロッカーで小荷物を配達するために計画された最大時間に対応し、運送業者の組織によって異なる場合がある。有効性持続時間は、サーバ管理者によって手動で設定されてもよく、または、リモート配送システムにおいて動作するプログラムによって調整または定義されてもよい。各認証子は、認証子の生成時にリモート配送システムによって生成される認証子識別情報316も含む。認証子識別情報は、リモート暗号化モジュール156によってランダムに生成され、他の認証子のために生成された他の認証子識別情報との類似性の確率は非常に低く、したがって、実質的に一意である。たとえば、32ビットのランダムな整数を生成するAES暗号化モジュールの場合、類似の確率は、40億回に1回よりも低い。そのような場合、リモート配送システムは、類似性をチェックし、すでに生成されている認証子識別情報を除く。好ましくは、認証子識別情報は一意であり、リモート配送システムは、ランダムで一意的認証子識別情報を生成するリモート暗号化モジュールを備えてもよい。

【0075】

リソース、および特にエネルギー消費を最小限に抑えるために、モバイルデバイスとの通信中または内部処理中にロックモジュールが認証子进行处理するために、認証子のサイズは最小である。特に、認証子には認証コードが含まれていない。認証コードは、一般的に、ロックモジュールからの要求に続いて、通信セッション内のメッセージの一部として交換される。

【0076】

モバイルデバイスとロックモジュールとの間のデータ交換を最小限に抑えるために、モバイルデバイスが特定のロックモジュールとの通信セッションを確立できるようにするために生成された認証子は、その特定のロックモジュールに対応するクラスタシークレットキーで暗号化される。モバイルデバイスとの通信セッションを許可するために、ロックモジュールは、認証子をチェックするためにそのシークレットキーを使用する。したがって、許可は特定のロックモジュールに対応するクラスタシークレットキーで実行される暗号化に基づいているので、モバイルデバイスによって特定の検証コードが提供される必要はない。

【0077】

モバイルデバイスがロックモジュールとの通信を確立するために認証子を送信すると、認証子が、次いでロックモジュールとの許可されていない通信を確立するために認証子を再利用する可能性がある許可されていない人によって捕捉される危険性がある。認証子のいかなる無許可の再利用をも防ぐために、ロックモジュールは、通信を確立するために認証子の使用を1回のみ許可する。ロックモジュールがモバイルデバイスによって提供される認証子に基づいてモバイルデバイスとの通信の確立を許可すると、ロックモジュールは

、認証子識別情報および認証子の有効期限をブラックリスト256に記憶し、関連付ける。その後、モバイルデバイスによって提供された認証子の認証子識別情報がブラックリスト256にすでに記憶されているとき、ロックモジュールは、接続を確立することを拒否し、結果として、ロックモジュールとモバイルデバイスとの間の切断となる。ロックモジュール内のデータストレージを最小限に抑えるために、有効期限に達すると、有効期限に関連付けられた認証子識別情報が、対応する有効期限とともに、ブラックリストから削除される。

【0078】

本発明は、区画へのアクセスを確保し、対応するロックモジュールとの通信を確保するための複数のチェックを提供する。第1に、ロックモジュールとの通信の確立は、ロックモジュールによって生成され、ロックモジュールに関連付けられた好ましくは一意のシークレットキーによる認証子の解読に基づいて許可される。次いで、認証子の妥当性が、その有効期限、およびそれがブラックリストを介してすでに使用されているかどうかに関してチェックされる。次いで、ユーザに付与された特権に基づいてアクション要求がチェックされる。さらに、モバイルデバイスとのロックモジュールによる通信セッションが許可されると、他のモバイルデバイスからの要求が拒否される。通信セッション中、モバイルデバイスからロックモジュールへの任意の要求は、認証子を含む必要があり、上記のチェックの各々が実行される。要求ごとに新しい認証子が必要になる場合がある。しかしながら、生成される認証子の数を最小限に抑えるために、通信セッション内のすべての要求に同じ認証子が使用され得る。この場合、認証子識別情報および関連する有効期限のブラックリストへの記憶は、モバイルデバイスによる接続解除時にロックモジュールによって実行される。

【0079】

システムセキュリティは、認証子の単一性または準単一性によっても改善される。リモート配送システムによって生成された各認証子は、ユーザカテゴリーに固有の特権マスク、認証子の作成の時間に固有の有効期限、および、リモート暗号化モジュールによってランダムに生成されるので実質的に一意の認証子識別情報を組み合わせる。さらに、各認証子は、特定のロックモジュールに実質的に一意のシークレットキーで暗号化される。したがって、各認証子は、実質的に一意である。認証子の単一性を確実にするために、リモート配送システムは、たとえば任意の類似の認証子識別情報を除くことによって、またはランダムで一意の認証子識別情報を生成することによって、一意の認証子識別情報を生成し得る。

【0080】

小荷物ロッカーの異なる区画の状況を監視し、記憶し、異なる区画を制御する中央制御ユニットを含む先行技術の小荷物ロッカーとは対照的に、自律区画で構成される本発明の小荷物ロッカーは、いかなる中央制御ユニットも含まない。本発明の小荷物ロッカーシステムでは、区画の状況の監視および記憶は、区画のローカル制御をMPLアプリケーションに委任するリモート配送システムによって実行される。必要なすべてのデータは、リモート配送システムによって小荷物ロッカーを操作するためにモバイルデバイスに送信される。特に、本発明の小荷物ロッカーへの小荷物の預け入れが運送業者によって開始されると、PL構成は、配送リモートサーバによって運送業者のMPLアプリケーションに提供される。PL構成は、小荷物ロッカーの区画に預けられている小荷物のすべてのクラスタ識別情報および小荷物識別情報を含む。PL構成は、たとえば、運送業者が小荷物を預けることができる区画を選択できるようにするためなど、ユーザがモバイルデバイスを介して小荷物ロッカーを操作できるようにするために不可欠である。好ましくは、PL構成は、区画クラスタからの最初のブロードキャストされたショートメッセージのモバイルデバイスによる受信に続いて、MPLアプリケーションによってリモート配送システムに要求される。

【0081】

ブロードキャストされたショートメッセージに含まれ、PL構成要求内でリモート配送システムに転送された一意のクラスタ識別情報250に基づいて、リモート配送システムは、

そのデータベースシステム130内で、対応する小荷物ロッカーを識別し、PL構成をモバイルデバイスに提供する。PL構成がモバイルデバイスによって受信されると、MPLアプリケーションによって預け入れに利用可能な区画が識別され、モバイルデバイスによって小荷物の預け入れのためのその区画を含む区画クラスタとの通信セッションが確立され得る。区画の利用可能性は、小荷物識別情報が区画クラスタの区画に関連付けられているかどうか、すなわち、区画識別に関連付けられているかどうかについて、リモート配送システムによって提供されるPL構成に含まれるクラスタステータステーブル136iに基づいて設定される。ブロードキャストされたショートメッセージにより区画クラスタから受信されたイベント制限252に基づいて、MPLアプリケーションは、PL構成の更新が必要であり得ることを設定する。代替実施形態では、運送業者が小荷物ロッカーの近くに到着する前に、PL構成がリモート配送システムから受信され、小荷物ロッカーのすべての区画クラスタからモバイルデバイスによってブロードキャストされたショートメッセージが受信される前に小荷物の預け入れを開始することができ、したがって、運送業者の遅延を最小限に抑える。

【0082】

PL構成に基づいて、MPLアプリケーションは、小荷物ロッカーを構成する区画クラスタの数を設定し、ブロードキャストされたショートメッセージが小荷物ロッカーのすべての区画クラスタから受信されることをチェックすることができる。運送業者による小荷物の預け入れの効率は、リモート配送システムによって提供されるPL構成の精度に依存する。したがって、小荷物ロッカーの区画に関連するイベントが、できるだけ早くリモート配送システムに転送されることが重要である。好ましくは、イベントは、ユーザのモバイルデバイスを介して小荷物ロッカーに対する任意のユーザ操作の一部として転送される。しかしながら、一部の小荷物の受取人は、モバイルデバイスを使用せずに小荷物を受け取る場合があり、または一部の操作では、イベントをモバイルデバイスに転送できない場合がある。したがって、預け入れなどのユーザ操作中または低電力状況などの区画クラスタ内部操作中の区画クラスタに関連する任意のイベントは、リモート配送システムへのイベントアップロードを実行する任意のモバイルデバイスを介して、リモート配送システムに転送され得るように、イベントテーブル255に記憶される。

【0083】

本発明の一態様では、本発明の小荷物ロッカーシステムによって、リモート配送システムと小荷物ロッカーの一部の区画クラスタとの間の非同期双方向マルチチャネル通信の確立が可能になり、複数のモバイルデバイスがマルチチャネルネットワークを構成する。モバイルデバイスと区画クラスタとの間の通信セッションの確立に続いて、たとえばイベントなどのデータを区画クラスタからリモート配送システムに転送するために、モバイルデバイスを介して区画クラスタからリモート配送システムの方角に、非同期通信が確立される。モバイルデバイスは、リモート配送システムへの転送が完了し得るまで、データを一時的に記憶する。この転送は、区画クラスタとの通信を確立する第1のモバイルデバイスを介してデータをアップロードできるように、小荷物ロッカーを操作するためのMPLアプリケーションがインストールされ、アクティブ化されている任意のモバイルデバイスを介して実行することができる。他の方向では、リモート配送システムは、モバイルデバイスを介して区画クラスタに、認証子などのデータ、または、たとえば、区画の操作をブロックするための命令を伝達する。区画クラスタへの転送が完了し得るまで、データまたは要求は、モバイルデバイスに一時的に記憶される。この非同期通信は、MPLアプリケーションがインストールされ、アクティブ化されている任意のモバイルデバイスを介して実行することができる。

【0084】

好ましくは、リモート配送システムは、あらかじめ設定されたルールに従って区画クラスタと通信するためのいくつかの好ましいモバイルデバイスを選択する。あらかじめ設定されたルールは、リモート配送システムから特定の区画クラスタへの通信が、小荷物の近日中の預け入れのためなど、特定の区画クラスタに関して、リモート配送システムに要求

しているモバイルデバイスのみ宛てられることであり得る。そのようなルールによって、リモート配送システムからの通信が、特定の区画クラスタとの通信を確立する可能性が最も高いモバイルデバイスのみを介してチャネリングされることが確実になる。双方向通信は、Webソケット技術に基づいて確立され得る。本発明によれば、小荷物ロッカーを操作するためのMPLアプリケーションがインストールされたモバイルデバイスは、リモート配送システムと区画クラスタとの間で通信するためのマルチチャネル非同期ネットワークを構成し、したがって、通信の効率を最適化しながら、本発明は、長距離ワイヤレス通信によってカバーされていないエリアにおける小荷物ロッカーの操作も可能にする。リモート配送システムからのデータまたは要求は、長距離ワイヤレス通信によってカバーされていないエリアに入る前に、モバイルデバイスに伝達され、一時的に記憶され得、区画クラスタからのデータは、リモート配送システムへの転送を完了するために、モバイルデバイスが長距離ワイヤレス通信によってカバーされていないエリアを出るまで、モバイルデバイスに一時的に記憶される。

10

【0085】

信頼できないモバイルデバイス、すなわち、MPLアプリケーションをダウンロードした任意のモバイルデバイスを介した非同期双方向マルチチャネル通信の確立には、上述の認証子およびチェックの使用を介して、本発明によって提供される強固なセキュリティプロセスが必要である。

【0086】

システムは、スマートフォンなどのモバイルデバイスを有する、または一部の小荷物の受取人が区画を操作するためにモバイルデバイスを所有していない、もしくは使用したくない場合があるので、モバイルデバイスのない小荷物の受取人によって操作されるように設計されている。小荷物の受取人は、短距離ワイヤレス通信機能を搭載していないモバイルデバイスを所有している場合があり、または、それをアクティブ化したくない場合がある。したがって、本発明の小荷物ロッカーシステムは、小荷物の受取人によって、モバイルデバイスによりリモートで、および、たとえば一意の認証コードを入力するためのピンパッドなどのロックインターフェースにより手動で操作することができる必要がある。しかしながら、モバイルデバイスにより小荷物ロッカーに自動的にアクセスすることは、本発明の主な目的であり、小荷物ロッカーに手動でアクセスすることは緩和手順である。モバイルデバイスにより小荷物ロッカーを操作することによって、認証コードを入力する必要がないので、優れたユーザ体験が提供される。本発明のこの好ましい態様の目的では、区画クラスタによるアクセス許可は、受取人のモバイルデバイスによって自動的に提供され、リモート配送システムによって最初に生成された認証子をチェックすることによって与えられる。

20

30

【0087】

手動アクセスの緩和手順をサポートするために、認証コードが各受取人に体系的に提供される。セキュリティ上の理由から、小荷物を受け取るために受取人に提供される認証コードは、ワンタイム認証コードを再度使用できないように、受け取られるべき特定の小荷物に一意に関連付けられている、ワンタイム認証コードであることが好ましい。ワンタイム認証コードは、リモート配送システムによって生成され、管理される。区画から受け取られる小荷物ごとに、受取人が小荷物を受け取るために来る前に、その区画を含む区画クラスタにワンタイム認証コードを提供する必要がある。一実施形態では、認証コードは、たとえば、小荷物に添付された小荷物識別情報をスキャンすることによって、預け入れのための小荷物が識別された後、運送業者による小荷物配達時に運送業者のMPLアプリケーションによって要求される。あるいは、別の実施形態では、認証コードは、リモート配送システムによって事前に生成され、運送業者が小荷物ロッカーへの毎日の配達を計画する前または計画するときに、一時的な記憶のためにMPLアプリケーションに伝達される。したがって、運送業者は、長距離ワイヤレス通信によってカバーされていないエリアに立っていても、小荷物ロッカーを操作することができる。

40

【0088】

50

認証コード要求を受信すると、リモート配送システムは、認証コードを生成し、認証コードは、モバイルデバイスに一時的に複製される。小荷物が預けられると、認証コードがモバイルデバイスから区画クラスタに転送され、小荷物が預けられた区画クラスタの区画に関連付けられ(すなわち、区画インデックス)、区画クラスタイベントのアップロードを介して、リモート配送システムに預け入れが通知される。次いで、リモート配送システムは、たとえば、SMSまたは電子メールを介して小荷物を受け取る必要があることを受取人に通知する。受取人がMPLアプリケーションをインストールしていない場合、通知は、受取人に、小荷物ロッカーの場所、区画識別子140j、および区画を開くために入力する必要がある認証コードを提供する。受取人がMPLアプリケーションをインストールしている場合、通知は、受取人に小荷物ロッカーの場所のみを通知し、区画を開くためにMPLアプリケーションを使用する必要があることを気づかせる。

10

【0089】

より一般的には、モバイルデバイスで小荷物ロッカーを操作する利点は、サイト所有者または運送業者を含む任意のユーザにも当てはまる。区画クラスタによるアクセス認証は、ユーザのモバイルデバイスによって自動的に提供され、リモート配送システムによって最初に生成される認証子をチェックすることによって与えられ、したがって、たとえば、キーパッドまたはバーコードのスキャンを介して手動認証入力を置き換える。

【0090】

前述のように新世代の小荷物ロッカーの必要性に応えることに加えて、本発明の自律区画クラスタは、追加の利点を提供する。区画クラスタロックモジュールが誤動作し、特に、それ以上通信できなくなった場合、誤動作した中央制御ユニットが小荷物ロッカー全体の動作をブロックし、直ちに介入する必要がある従来の小荷物ロッカーとは異なり、他のすべての区画クラスタは、引き続き操作され、通信することができる。本発明の小荷物ロッカーでは、最も適切なときに、誤動作した区画クラスタの単純な交換を行うことができる。本発明の別のユーザの利点は、各ユーザが自分のモバイルデバイスで本発明の区画クラスタを操作し、それによって、複数のユーザがいくつかの区画クラスタに並行してアクセスできることである。忙しい期間中、複数の受取人が小荷物を並行して受け取るか、さらには運送業者および受取人が小荷物ロッカー区画クラスタと並行して対話する場合がある。そのような並列動作は、ショートメッセージをブロードキャストし、動作イベントを記憶し、モバイルデバイスおよびリモート配送システムのPL構成情報を更新するロックモジュールを提供する本発明のシステムアーキテクチャによって可能になる。

20

30

【0091】

図4は、ロックモジュールをセットアップするための本発明の一実施形態を示す。セットアップの主な目的は、リモート配送システム106と小荷物ロッカーのロックモジュール120iとの間で交換されるデータを暗号化し、解読するため、特に、認証子を暗号化し、解読するために、シークレットキーの機密性の高い安全な転送を確実にすることである。本発明によれば、セットアップは、スマートフォンまたはPDAなど任意のモバイルデバイスを介して実行することができ、したがって、小荷物ロッカーが設置されている場所の現場を含むどこでも行うことができる。しかしながら、セットアップが倉庫またはカスタマイズセンターで実行されるとき、一般的に、現場に設置する前の最終出荷の直前に、ロックモジュールの短距離通信機能と互換性のある短距離ワイヤレス通信機能を有する、PCまたはラップトップなどの固定のコンピュータ化されたデバイスを介してセットアップを実行することもできる。モバイルデバイス(または固定のコンピュータ化されたデバイス)にインストールされたMPLアプリケーションは、ロックモジュールのセットアップを実行するための資格証明書を有するユーザカテゴリーに従ってインスタンス化され、セットアップを実行するためのすべての機能が、モバイルアプリケーションにおいてユーザから利用できるようになる。好ましくは、ユーザは、小荷物ロッカーのすべてのロックモジュールをカバーし得るセットアップを実行するためのウィザードプログラムを通して案内される。

40

【0092】

ステップ402で、ユーザは、セットアップに必要なMPLアプリケーション機能にアクセ

50

スするためにモバイルデバイスにおいてログインを実行することによって、ロックモジュールのセットアップを開始する。ログイン手順では、ユーザ識別情報および/またはユーザの個人パスワードを含み得、モバイルデバイスインターフェースを介した手動入力(たとえば、モバイルデバイスのキーパッドまたはタッチスクリーンに識別子をキー入力することによるなど)など、当技術分野で知られている任意の手段を介して捕捉され得るユーザの資格証明書の捕捉、モバイルデバイスによる識別バーコード読み取り、またはイメージングまたはバイオメトリ技術または無線周波数技術を介したモバイルデバイスによる識別の捕捉を必要とする。モバイルアプリケーションは、ユーザの資格証明書を含むログイン要求をリモート配送システムに送信する。ログイン要求、および特にデータベースシステム130に記憶されている資格証明書に基づいてユーザ資格証明書を検証した後、リモート配送システムは、ユーザのモバイルデバイス上のMPLアプリケーションセットアップ機能へのアクセスを許可する。

【0093】

ログインに続いて、MPLアプリケーションは、ユーザカテゴリーに従ってインスタンス化され、ユーザは、ロックモジュールのセットアップを開始するためのセットアッププログラムを選択する(ステップ404)。モバイルデバイスは、シークレットキー254の送信を安全にするためにリモート配送システムに対して公開鍵152を要求する(ステップ406)。リモート配送システムがまだ公開鍵を生成していない場合(ステップ408)、リモート配送システムは、いくつかの公開鍵152および対応する秘密鍵154を生成し、これらの公開鍵および秘密鍵をデータベース130に記憶し、関連付ける(ステップ410)。これらの公開鍵および秘密鍵は、ロックモジュールからリモート配送システムに、暗号化された形式でシークレットキーを転送するために使用される。これらは、リモート配送システムによって定期的に変更される場合がある。たとえば、セットアップされるべき小荷物ロッカーごとに、新しい対の公開鍵と秘密鍵が生成されてもよい。ステップ412で、リモート配送システムは、公開鍵をモバイルデバイスに送信し、モバイルデバイスはそれを一時的に記憶する。ステップ414で、モバイルデバイスは、ロックモジュールとの第1の接続を実行する。モバイルデバイスは、ロックモジュールに関連付けられた一意のクラスタ識別情報250を含むブロードキャストされたショートメッセージをロックモジュールから受信するとすぐに、ロックモジュールとの第1の接続を確立するための要求を送信する。この第1の接続要求は、いかなる認証子も備えておらず、ロックモジュールの不揮発性メモリ240にシークレットキーが記憶されていない場合に許可される。第1の接続要求を検証した後、ロックモジュールは、モバイルデバイスと短距離ワイヤレス通信を確立する。次いで、モバイルデバイスは、ロックモジュールにシークレットキーの生成を要求し、公開鍵を転送する(ステップ416)。好ましくは、交換の回数を最小限に抑えるために、また、公開鍵が送信されたかどうかに関するチェックが行われる必要がないように、シークレットキーの生成の要求および公開鍵の転送が同じ要求内に含まれる。シークレットキー生成要求は、認証子を含まずに許可され得る第1の接続要求を含む唯一の要求である。シークレットキー生成要求を検証した後、ロックモジュールの

不揮発性メモリ240にシークレットキーがまだ記憶されていないことをチェックすることによって、ロックモジュールは、好ましくは、一意のシークレットキー254を生成し、それを不揮発性メモリ240にローカルに記憶する(ステップ418)。シークレットキーは、他のロックモジュールによってランダムに生成された鍵との非常に低い確率の類似性で暗号化モジュール256によってランダムに生成され得、したがって、実質的に一意である。そのような場合、リモート配送システムは、類似性をチェックし、シークレットキーの単一性を保証するようにいくつかのシークレットキーの変更を指示する。好ましくは、ロックモジュールは、ランダムで一意のシークレットキーを生成する暗号化モジュールを備える。好ましい実施形態では、ロックモジュールは、暗号化された形式でシークレットキーを記憶する。ステップ420では、ロックモジュールは、シークレットキーを公開鍵で暗号化し、暗号化されたシークレットキーをモバイルデバイスに送信する。

【0094】

ステップ422で、モバイルデバイスは、ロックモジュールの登録のためにリモート配送システムに要求を送信し、暗号化された形式でシークレットキーを送信する。それによって、シークレットキーの生成は安全にされ、機密性が高く、シークレットキーは、モバイルデバイスを介して安全かつ機密に転送される。登録要求を検証した後、特に、その特定のロックモジュールについてリモート配送サーバのデータベースシステム130にまだシークレットキーが記録されていないことをチェックすることによって、リモート配送システムは、送信された暗号化されたシークレットキーを秘密鍵で解読し、ロックモジュールを登録する(ステップ424)。登録の一部として、ロックモジュールに送信されるべきデータの暗号化、特に、認証子の暗号化、およびロックモジュールから受信されたデータの解読のためにシークレットキーを後で使うことができるように、リモート配送システムは、好ましくは暗号化された形式でシークレットキーをクラスタシークレットキー136iとして記憶し、クラスタシークレットキーをデータベース130においてロックモジュール(すなわち一意のクラスタ識別情報134i)に関連付ける。

【0095】

ロックモジュールへの第1の接続後、およびシークレットキーの送信後、モバイルデバイスからロックモジュールへの新しい要求は、リモート配送システムによって生成され、ロックモジュールに対応するクラスタシークレットキーで暗号化された認証子を含める必要がある。通信を安全にすることに加えて、各要求に認証子を含めることによって、ロックモジュールは、ロックモジュールに宛てられた各要求が提供されるので、認証子を記憶する必要がなくなる。特に、(たとえばセキュリティ上の理由で)新しいシークレットキーの生成が必要とされる場合、ロックモジュールに宛てられた要求は、ロックモジュールに現在関連付けられているクラスタシークレットキーで暗号化された認証子を含む。

【0096】

セットアップ手順中に、シークレットキーの送信後、切断タイムアウト258やクラスタブロードキャストテーブル272など、他のパラメータがリモート配送サーバからロックモジュールに転送される。この送信は、認証子を含む要求を介して実行され得る。切断タイムアウトは、セットアップの前にリモート配送サーバ上に構成され、30秒から30分の間で設定されてよく、一般的に、5分が最大である。必要に応じて、リモート配送サーバによってモバイルデバイスを介してロックモジュールに送信される命令を介して、切断タイムアウトを後で変更してもよい。

【0097】

図5は、ロックモジュールによるモバイルモジュールからの要求の検証のための本発明の一実施形態を示す。モバイルデバイスが小荷物ロッカーのロックモジュールに要求を送信するたびに、ロックモジュールとの通信および小荷物ロッカーの区画へのアクセスを安全にするために、以下のステップが適用される。このプロセスは、特に、ロックモジュールとの通信を確立するためのモバイルデバイスからの要求の場合に適用される。

【0098】

ロックモジュールの登録が完了すると、モバイルデバイスからロックモジュールへの任意の要求は、ロックモジュールとの短距離ワイヤレス通信を確立するための少なくとも1つの認証子を要求し、受信するためのリモート配送システムへのモバイルデバイスのログインが先行するものとする。好ましくは、一意にロックモジュールに対応するクラスタシークレットキー136iで暗号化された認証子300を含む要求は、モバイルデバイスによってロックモジュールに送信される(ステップ510)。要求は、ロックモジュールによってサポートされる機能(または機能のグループ)に関連付けられ、要求が検証されると、機能(または機能のグループ)はロックモジュールによって実行される。好ましくは、要求は、ロックモジュール内のコードの複雑さを最小限に抑える、または要求のサイズを最小限に抑えるために、1つの機能のみに対応する。しかしながら、キャリアプロセスおよび小荷物ロッカーシステムの構成に応じて、交換の回数を最小限に抑えるために、要求内のいくつかの機能をグループ化することが必要になる場合がある。認証子は、区画インデックス310、ロックモジュールに関するユーザ権利を定義する特権マスク312、有効期限314、および

一意の認証子識別情報316を含む。ステップ512で、ロックモジュールは、認証子を暗号化するためにリモート配送システムによって使用されるクラスタシークレットキーと一致するシークレットキー254で認証子を解読する。この解読のポジティブチェックは、要求を許可するための第1のステップである(ステップ514)。この第1のチェックは、好ましくは、解読された認証子の形式および内容を検証することによって実行される。そのような方法によって、認証子および要求の最小サイズが保証される。あるいは、この第1のチェックは、暗号化された認証子に含まれる暗号ソルトを識別する、または認証子に添付されたハッシュなどの署名を、ロックモジュールにインストールされた暗号アルゴリズムによって解読された認証子に基づいて計算され、リモート配送サーバにインストールされ、認証子に添付されたハッシュを暗号化した暗号化アルゴリズムに対応する署名と比較することによって実行され得る。しかしながら、これらの方法は、より大きいサイズの要求をもたらす。解読のネガティブチェックの場合、ロックモジュールは、解読除外メッセージをモバイルデバイスに返す(ステップ516)。認証は、特定のロックモジュールに対応するクラスタシークレットキーを使用した認証子の正常な解読に基づき、モバイルデバイスによって特定の検証コードが提供される必要はない。ステップ518で、ロックモジュールは、認証子識別情報316がブラックリスト256に記憶された認証子識別情報と一致するかどうかをチェックする。一致の場合(すなわち、認証子がブラックリストに記載されている場合)、ロックモジュールは、モバイルデバイスにブラックリスト除外メッセージを返す(ステップ520)。認証子がブラックリストに記載されていない場合、ロックモジュールはステップ522に進み、有効期限314がチェックされる。有効期限に達した場合、認証子は、もはや有効ではなく、ロックモジュールは、有効期限除外メッセージをモバイルデバイスに返す(ステップ524)。そうでない場合、ロックモジュールはステップ526に進み、ロックモジュールは、要求の対象となる機能(または機能のグループ)がユーザに許可されているかどうかを検証する。ロックモジュールは、機能テーブル260内の要求の対象となる機能(または機能のグループ)を識別し、機能(または機能のグループ)が特権マスク312によって許可されているかどうかをチェックする。機能(または機能のグループ)が特権マスクによって許可されていない場合、ロックモジュールは、機能除外メッセージをモバイルデバイスに返す(ステップ528)。そうでない場合、ロックモジュールは要求を許可し、要求に従って続行する(ステップ530)。上記の除外のいずれかが発生するたびに、要求は、ロックモジュールによって許可されない(ステップ532)。有効期限、ブラックリスト、または特権の上記のチェックは、任意の順序で実行することができる。

【0099】

要求ごとに新しい認証子が必要とされる場合、要求の完了後、ロックモジュールは、認証子識別情報および現在使用されている認証子の関連する有効期限をブラックリストに記憶する。しかしながら、生成される認証子の数を最小限に抑えるために、通信セッション内のすべての要求に同じ認証子を使用され得る。この場合、認証子識別情報および関連する有効期限のブラックリストへの記憶は、モバイルデバイスからの切断要求に従ってロックモジュールによって実行される。モバイルデバイスとロックモジュールとの間の短距離ワイヤレス通信が意図せずに切断された場合、切断タイムアウト258に達した後、認証子識別情報および使用されている最新の認証子の関連する有効期限がブラックリストに記憶される。好ましくは、意図しない切断の場合、生成された認証子の数を最小限に抑えるために、切断タイムアウト258に達する前に、モバイルデバイスは、ロックモジュールとの接続を再確立するために同じ認証子を使用することができる。切断タイムアウトに達するためのカウントダウンは、ロックモジュールによって受信された最新の要求の後に開始され、すなわち、ロックモジュールによって受信されたすべての検証された要求の後にカウントダウンが再開される。

【0100】

本発明の特定の実施形態では、モバイルデバイスが、小荷物ロッカーの隣にローカルに設けられてもよい。このローカルモバイルデバイスは、すべてのユーザが小荷物ロッカーを操作するために使用することができる。特に、いかなるスマートフォンのない小荷物の

10

20

30

40

50

受取人または機能不全のモバイルデバイスを有する任意の運送業者によって使用されてもよい。また、ローカルモバイルデバイスは、小荷物の配達に使用するモバイルデバイスにMPLアプリケーションを一時的または永続的に統合することを望まない運送業者組織によって使用されてもよい。MPLアプリケーションは、最終的に小荷物ロッカーの現場の設置時にリモートサーバからのダウンロードを介してローカルモバイルデバイスにインストールされ、ユーザがローカルモバイルデバイスにログオンすると、ユーザカテゴリに従ってインスタンス化される。ローカルモバイルデバイスは、前述のモバイルデバイスのネットワークと並行して操作されてもよく、または、一部の用途では、モバイルデバイスのネットワークを簡単に置き換え得る。一実施形態では、ローカルモバイルデバイスは、小荷物ロッカーの隣の台座、または小荷物ロッカーの隣の壁に取り付けられた、もしくは小荷物ロッカーの区画クラスタに直接取り付けられたブラケットに固定して取り付けられる。ローカルモバイルデバイスは、ロックモジュールと同様の自律手段で電力供給され得る。一部の用途では、ローカルモバイルデバイスは、利用可能になったときにローカル電気ネットワークに接続される場合がある。しかしながら、区画クラスタは、小荷物ロッカーを簡単に設置し、区画を簡単に交換したり、現場で小荷物ロッカーの構成を簡単にアップグレードまたは変更したりするために、自立型のままである。最終的に、ローカルモバイルデバイスは、同じエリアにある複数の小荷物ロッカーを操作することができる。好ましい実施形態では、ローカルモバイルデバイスが、短距離通信機能をサポートする既存の小荷物ロッカーに組み込まれてもよい。

【0101】

上述の本発明の小荷物ロッカーシステムおよび方法は、一緒に組み立てられた自律区画クラスタで構成される小荷物ロッカーを含む。しかしながら、本発明の別の実施形態では、単一の区画クラスタが、小荷物ロッカーの一部として組み立てられることなく、単独でスタンドアロン構成で使用されてもよく、または単一の区画、すなわち、単一の区画を含む単一の区画クラスタが、スタンドアロン構成で単独で使用されてもよいことを当業者は容易に理解する。そのような単一のスタンドアロン区画クラスタまたは単一のスタンドアロン区画は、宅配またはシングルポイント配達システム(single point delivery system)に使用されてもよい。本発明の別の実施形態では、区画クラスタを、それ自体のロックモジュールを備えた単一の区画に縮小し、小荷物ロッカーの一部として組み立てることができることも当業者には容易に理解できる。そのようなアーキテクチャは、クラスタに組み込まれた複数の区画に単一のロックモジュールを使用することによるコスト削減の恩恵は受けないが、よりモジュール式でより柔軟性の高いソリューションを提供する。

【符号の説明】

【0102】

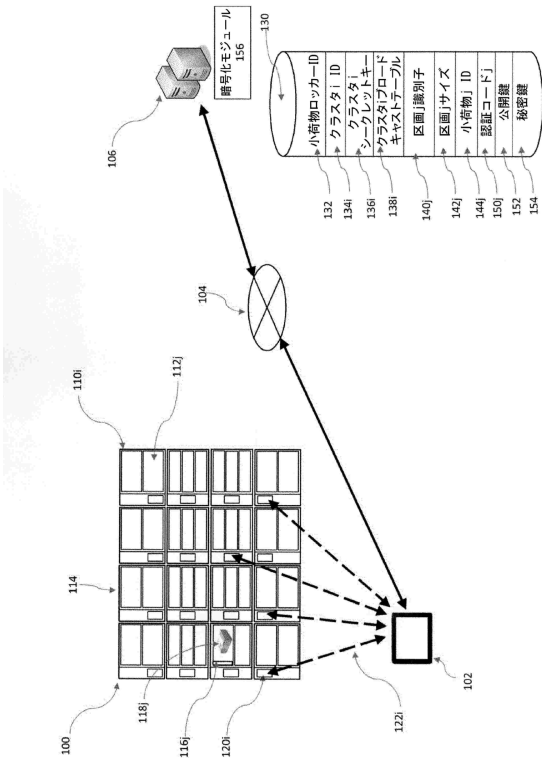
- 10 電子小荷物ロッカー
- 20 長距離通信ネットワーク
- 25 リモート配送システム
- 30i 区画
- 32 中央制御ユニット
- 34 タッチスクリーン
- 36 バーコードリーダー
- 38 識別
- 40 小荷物
- 42 列
- 100 小荷物ロッカー
- 102 モバイルデバイス
- 104 長距離通信ネットワーク
- 106 リモート配送システム
- 110i 自律区画クラスタ
- 112j 区画

114	列	
116j	ヒンジ付きドア	
118j	小荷物	
120i	通信ロックモジュール	
122i	短距離ワイヤレス通信	
130	データベースシステム	
132	小荷物ロッカー識別	
134i	クラスタ識別情報	
136i	クラスタシークレットキー	
136i	クラスタステータステーブル	10
138i	クラスタブロードキャストテーブル	
140j	区画識別子	
142j	区画サイズ	
144j	小荷物識別情報	
150j	認証コード	
152	公開鍵	
154	秘密鍵	
156	リモート暗号化モジュール	
210	プロセッサ	
210A	高エネルギープロセッサモジュール	20
210B	低エネルギープロセッサモジュール	
210C	非常に低いエネルギープロセッサモジュール	
212	揮発性メモリ	
214	バス	
216	無線トランシーバモジュール	
218	アンテナ	
220n	電気錠	
221	電力段	
222n	センサー	
223	センサー入出力ポート(I/O)	30
224n	視覚インジケータ	
225	インジケータ入出力ポート(I/O)	
226	ロックインターフェース	
228	電源	
230	エネルギー管理モジュール	
240	不揮発性メモリ	
250	クラスタ識別情報	
252	イベント制限	
252n	区画インデックス	
254	シークレットキー	40
255	イベントテーブル	
256	ブラックリスト	
256	暗号化モジュール	
258	切断タイムアウト	
260	機能テーブル	
270n	認証コード	
272	クラスタブロードキャストテーブル	
280	低エネルギースリープタイマー	
282	リスニング時間ウィンドウタイマー	
300	認証子	50

- 310 区画インデックス
- 312 特権マスク
- 314 有効期限
- 316 認証子識別情報

【図面】

【図 1】



フロントページの続き

ボン・５４

(72)発明者 トマ・エロー

フランス・８４０００・アヴィニョン・ブルヴァール・カブドヴィラ・６・ビス

(72)発明者 アルノー・イヴォ

フランス・８４３００・タイヤール・ロト・マス・サン・ジャン・４

審査官 吉田 歩

(56)参考文献 国際公開第２０１７／１６３０１８（WO，A２）

特開２００６－０５００２０（JP，A）

特開２０１８－０５７８６６（JP，A）

特開２０１６－１３７９６３（JP，A）

特開２０１３－１６１２１７（JP，A）

特開２０１８－１８９６３０（JP，A）

特開２０１６－０５３８７９（JP，A）

特開２００８－０２７１８２（JP，A）

(58)調査した分野 (Int.Cl.，DB名)

G 0 6 F 2 1／3 5

G 0 6 F 2 1／4 4

G 0 6 F 2 1／3 3