



(11)

EP 3 195 276 B1

(12)

FASCICULE DE BREVET EUROPEEN

(45) Date de publication et mention
de la délivrance du brevet:

09.10.2024 Bulletin 2024/41

(21) Numéro de dépôt: **15771671.3**

(22) Date de dépôt: **27.08.2015**

(51) Classification Internationale des Brevets (IPC):
G07C 9/00 (2020.01)

(52) Classification Coopérative des Brevets (CPC):
G07C 9/00896; G07C 9/00571

(86) Numéro de dépôt international:
PCT/FR2015/052283

(87) Numéro de publication internationale:
WO 2016/042232 (24.03.2016 Gazette 2016/12)

(54) **DISPOSITIF DE DEVERROUILLAGE D'AU MOINS UN OUVRANT ET EQUIPEMENT DE
RECEPTION D'OBJETS, ENSEMBLE DE STOCKAGE DE DONNEES ET SYSTEME DE
DISTRIBUTION D'OBJETS ASSOCIES**

VORRICHTUNG ZUM ENTRIEGELN VON WENIGSTENS EINEM ÖFFNUNGSBLATT UND
VORRICHTUNG ZUR AUFNAHME VON OBJEKTEN, ZUGEHÖRIGE
DATENSPEICHERANORDNUNG UND ZUGEHÖRIGES OBJEKTVERTEILUNGSSYSTEM

DEVICE FOR UNLOCKING AT LEAST ONE OPENING LEAF AND EQUIPMENT FOR RECEIVING
OBJECTS, ASSOCIATED DATA STORAGE ASSEMBLY AND ASSOCIATED OBJECT
DISTRIBUTION SYSTEM

(84) Etats contractants désignés:
**AL AT BE BG CH CY CZ DE DK EE ES FI FR GB
GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO
PL PT RO RS SE SI SK SM TR**

(30) Priorité: **16.09.2014 FR 1458753**

(43) Date de publication de la demande:
26.07.2017 Bulletin 2017/30

(73) Titulaire: **LA POSTE
75015 Paris (FR)**

(72) Inventeur: **FABRE, Jean-Paul
F-75014 Paris (FR)**

(74) Mandataire: **Novagraaf Technologies
Bâtiment O2
2, rue Sarah Bernhardt
CS90017
92665 Asnières-sur-Seine Cedex (FR)**

(56) Documents cités:
**WO-A1-2009/018931 WO-A1-2012/143634
WO-A1-2013/189721 DE-A1- 10 164 574**

EP 3 195 276 B1

Il est rappelé que: Dans un délai de neuf mois à compter de la publication de la mention de la délivrance du brevet européen au Bulletin européen des brevets, toute personne peut faire opposition à ce brevet auprès de l'Office européen des brevets, conformément au règlement d'exécution. L'opposition n'est réputée formée qu'après le paiement de la taxe d'opposition. (Art. 99(1) Convention sur le brevet européen).

Description

DOMAINE TECHNIQUE DE L'INVENTION

[0001] La présente invention concerne le domaine des dispositifs de déverrouillage d'un ouvrant formant accès à une zone, tel que par exemple un ouvrant de consigne ou de boîte aux lettres. De tels dispositifs permettent de sécuriser l'accès à la zone, par exemple au contenu de la consigne ou de la boîte aux lettres. Plus particulièrement, l'invention concerne les dispositifs de déverrouillage commandés électroniquement au moyen d'un objet portatif tel qu'un téléphone mobile équipé de moyens de couplage au dispositif de déverrouillage.

ETAT DE LA TECHNIQUE ANTERIEURE

[0002] Il existe de nombreux dispositifs permettant d'assurer la fermeture et le déverrouillage d'un ouvrant formant accès à une zone.

[0003] Notamment, le document EP 2 628 418 A1 décrit un dispositif de déverrouillage d'un ouvrant d'une consigne de réception d'un objet. Le dispositif est équipé d'une serrure électronique apte à verrouiller automatiquement l'ouvrant lors de la fermeture manuelle de celui-ci, et à déverrouiller l'ouvrant suite à la réception d'un signal émis par une carte à puce électronique. Un inconvénient de ce dispositif est que la carte à puce peut être perdue ou volée, ou encore compromise par duplication, ce qui nuit à la sécurité de l'ensemble et peut permettre à une personne non autorisée d'accéder facilement au contenu de la consigne.

[0004] D'autres dispositifs sont connus, qui intègrent des moyens d'acquisition de données permettant par exemple la saisie d'un code alphanumérique par l'utilisateur pour provoquer le déverrouillage de l'ouvrant. Une problématique rencontrée dans de tels dispositifs, outre l'aspect contraignant de la saisie manuelle du code, est là encore celle du vol possible du code par une personne mal intentionnée.

[0005] Une solution connue pour pallier en partie l'inconvénient précité est proposée par des dispositifs permettant de sécuriser un accès à une zone à partir d'une clef numérique transmise par un téléphone portable. De tels dispositifs comprennent une mémoire stockant une liste de clefs numériques prédéterminées autorisant le déverrouillage de l'ouvrant.

[0006] Toutefois, la sécurité relative au déverrouillage par un tel dispositif peut être compromise si un utilisateur non autorisé utilise une ou plusieurs clefs numériques ayant déjà servies et appartenant à la liste de clefs numériques prédéterminées. En outre, un tel dispositif impose une maintenance relativement complexe et coûteuse, notamment pour mettre à jour à tout instant, dans la mémoire du dispositif, la liste des clefs numériques « valables ».

[0007] Le document WO 2009/018931 A1 divulgue un système de compartiments munis de dispositifs de ver-

rouillage permettant une ouverture et une fermeture automatique des ouvrants donnant accès aux compartiments, pour éviter à un utilisateur d'avoir à fermer ou à ouvrir manuellement les ouvrants respectifs.

[0008] Le document WO 2013/189721 A1 divulgue un cadenas électronique permettant le verrouillage et le déverrouillage d'appareils électriques munis d'emplacements dédiés pour le cadenas.

[0009] Le document DE 10164574 divulgue un dispositif de déverrouillage d'un ouvrant comprenant une serrure électronique et un module de commande relié à la serrure électronique.

[0010] Il est également connu du document WO2012/143634A1 de prévoir un dispositif de contrôle d'accès de casiers, dans lequel, à chaque fermeture de la porte de casier, une clé logique comprenant un nombre pseudo-aléatoire est générée. Cette clé est enregistrée et transmise à une carte à puce. Le déverrouillage de la porte du casier est permis si concordance est faite entre la clé logique contenue dans la carte à puce et celle enregistrée lors du verrouillage.

EXPOSE DE L'INVENTION

[0011] L'invention décrite par la suite vise à remédier à tout ou partie des inconvénients de l'état de la technique et notamment à proposer un dispositif de déverrouillage d'au moins un ouvrant formant accès à une zone permettant d'assurer de manière simple et fiable la fermeture et le déverrouillage de l'ouvrant, tout en améliorant le niveau de sécurité du dispositif.

[0012] A cet effet, l'invention a pour objet un système de distribution d'objets comprenant :

- au moins un équipement de réception d'objets, le ou chaque équipement comprenant au moins une consigne munie d'un ouvrant formant accès à un espace intérieur de la consigne destiné à recevoir un objet, l'équipement comprenant en outre un dispositif de déverrouillage de l'ouvrant, une serrure électronique étant agencée au sein de la consigne, le dispositif de déverrouillage comprenant la serrure électronique et un module de commande relié à la serrure électronique via une liaison de données, la serrure électronique comprenant des moyens moteurs aptes à verrouiller et déverrouiller l'ouvrant suivant la valeur d'une consigne reçue via la liaison de données, le module de commande comprenant un capteur d'un signal comprenant une clef numérique et un composant électronique de reconnaissance permettant d'authentifier la clef numérique, le capteur étant propre à transmettre le signal au composant électronique de reconnaissance, ledit composant électronique de reconnaissance étant relié à la liaison de données et étant alimenté par des moyens d'alimentation électrique, l'authentification de la clef numérique par le composant électronique de reconnaissance générant un signal de consigne de dé-

sactivation des moyens moteurs pour le déverrouillage de l'ouvrant, la serrure électronique comprenant des moyens de détection d'une fermeture de l'ouvrant aptes à émettre un signal de détection de fermeture sur la liaison de données, le module de commande comprenant en outre des moyens d'émission d'un signal et des moyens de génération de clefs numériques reliés aux moyens d'alimentation électrique, au composant électronique de reconnaissance et aux moyens d'émission, les moyens de génération étant propres à générer une clef numérique unique à chaque fermeture de l'ouvrant, le signal émis comportant la clef numérique unique générée, le composant électronique de reconnaissance étant propre à authentifier la clef numérique reçue par comparaison avec la clef numérique unique générée ;

- deux dispositifs de communication propre à émettre un signal comprenant une clef numérique, le signal étant apte à être capté par le capteur du ou d'un des dispositif(s) de déverrouillage et analysé par le composant électronique de reconnaissance dudit dispositif de déverrouillage, chaque dispositif de communication comprenant des moyens de réception de données adaptés pour communiquer avec les moyens d'émission du dispositif de déverrouillage de sorte à recevoir la ou les clef(s) numérique(s) générée(s) par le module de commande dudit dispositif ;
- un ensemble de stockage de données, relié à chaque dispositif de communication via un réseau de communication, l'ensemble de stockage de données étant propre à stocker au moins une clef numérique destinée, après analyse par le composant électronique du module de commande, à déverrouiller la ou une des consigne(s) de l'équipement de réception d'objets,

le système de distribution étant caractérisé en ce que l'ensemble de stockage est propre à transmettre, à un premier desdits dispositifs de communication, la ou chaque clef numérique fournie par un deuxième desdits dispositifs de communication, et, pour la ou chaque clef numérique reçue, à générer un message de notification indicatif de la présence d'un objet dans la ou une des consigne(s) et à transmettre ce message de notification au premier dispositif de communication, et

en ce que le composant électronique est propre, pour chaque consigne, à remplacer dans l'ensemble de stockage de données une éventuelle clef numérique déjà stockée par la clef numérique unique nouvellement générée lors de la fermeture de l'ouvrant de la consigne.

[0013] Grâce à la présence de moyens de détection d'une fermeture de l'ouvrant au sein de la serrure élec-

tronique et de moyens de génération d'une clef numérique unique au sein du module de commande, et au fait que le composant électronique de reconnaissance est propre à authentifier la clef numérique reçue par comparaison avec la clef numérique unique générée, le risque qu'une personne non autorisée compromette la zone en utilisant une ou des clef(s) ayant déjà servie(s) est fortement réduit. Ceci permet d'obtenir un haut niveau de sécurité et d'ainsi pouvoir par exemple attribuer à un utilisateur identifié l'usage temporaire ou non de la zone, par fourniture à cet utilisateur de la clef numérique générée. Le dispositif de déverrouillage selon l'invention permet ainsi avantageusement de s'assurer que seul l'utilisateur identifié, ou un des mandataires qu'il a préalablement désignés, est à même de déverrouiller l'ouvrant pour accéder à la zone.

[0014] Le deuxième dispositif de communication permet ainsi de transmettre à l'ensemble de stockage la clef numérique générée par le dispositif de déverrouillage. L'ensemble de stockage de données peut ensuite transmettre cette clef numérique au premier dispositif de communication, correspondant à un dispositif de communication d'un destinataire prédéterminé de l'objet, un identifiant de ce premier dispositif de communication ayant de préférence été préalablement pré-enregistré dans l'ensemble de stockage.

[0015] Selon une caractéristique technique particulière de l'invention, le module de commande comprend en outre un composant de codage de données connecté d'une part entre le capteur et le composant électronique et d'autre part entre les moyens de génération de clefs numériques et les moyens d'émission d'un signal, le composant de codage étant propre à coder les clefs numériques générées par les moyens de génération et à transmettre les clefs numériques codées aux moyens d'émission, le composant de codage étant propre à décoder une clef numérique codée contenue dans un signal reçu par le capteur et à transmettre la clef numérique décodée au composant électronique.

[0016] Ceci permet d'augmenter le niveau de confidentialité des clefs générées, notamment en cas de vol de celles-ci après leur émission par les moyens d'émission. Le niveau de sécurité global du dispositif est ainsi amélioré.

[0017] Avantageusement, le composant électronique comprend une horloge électronique, une information d'horodatage est associée à la clef numérique unique générée, et le composant électronique n'est propre à authentifier une clef numérique reçue par comparaison avec la clef numérique unique générée que pendant une durée prédéterminée.

[0018] Cette caractéristique permet de réduire le risque de compromission de l'accès à la zone en cas de vol, après son émission, d'une clef numérique générée. Un gain de sécurité supplémentaire est ainsi obtenu.

[0019] Dans une réalisation particulière de l'invention, le module de commande est agencé au sein de la consigne. Selon cette réalisation particulière de l'invention,

l'encombrement de l'équipement de réception d'objets est réduit.

[0020] Dans une autre réalisation particulière de l'invention, l'équipement de réception d'objets comprend une pluralité de consignes, chaque consigne étant munie d'un ouvrant, et le dispositif de déverrouillage comprend une pluralité de serrures électroniques, chaque serrure électronique étant agencée au sein d'une des consigne(s) et étant apte à verrouiller et déverrouiller l'ouvrant de cette consigne, le module de commande étant relié à chaque serrure électronique via une liaison de données et étant propre à générer une clef numérique unique à chaque fermeture d'un des ouvrants.

[0021] Cette autre réalisation particulière de l'invention permet, grâce à la mutualisation du module de commande relié à plusieurs serrures électroniques, de centraliser l'accès au dispositif de déverrouillage des ouvrants des consignes. Les coûts sont ainsi réduits.

[0022] Selon une caractéristique technique particulière de l'invention, l'ensemble de stockage de données comprend un module de gestion de la disponibilité des consignes, le module comportant une table de stockage d'une pluralité de bulletins de consignation, chaque bulletin de consignation étant associé à l'une des consignes et étant apte à prendre une première valeur correspondant à un état libre de la consigne, et une deuxième valeur correspondant à un état occupé de la consigne.

[0023] Grâce à cette caractéristique, une mutualisation de l'accès à la consigne est ainsi possible, par réservation séquentielle de la consigne à différents utilisateurs, sans risque quant à la confidentialité des objets déposés. Ceci permet ainsi une réduction de l'encombrement de l'équipement de réception d'objets et donc une réduction des coûts.

[0024] Selon une caractéristique technique particulière de l'invention, le premier dispositif de communication est muni de moyens d'acquisition de données comprenant une interface utilisateur et une application stockée au sein du premier dispositif de communication.

[0025] Avantageusement, l'ensemble de stockage est propre à être relié, via le réseau de communication, à une base de données de destinataires, la base de données de destinataires comprenant des enregistrements préalablement validés comme des valeurs d'authentification de destinataires, et les moyens d'acquisition de données du premier dispositif de communication sont propres, via l'interface utilisateur, à recevoir une entrée d'identification d'un utilisateur, l'ensemble de stockage étant propre à transmettre, au premier dispositif de communication, la ou chaque clef numérique reçue uniquement si l'entrée d'identification correspond à un des enregistrements de la base de données de destinataires.

[0026] Ceci permet une authentification plus sûre de l'identité du destinataire, préalablement à la remise de la clef numérique à ce destinataire via son dispositif de communication. Le niveau de sécurité global du système de distribution d'objets est ainsi amélioré.

[0027] Selon un autre aspect, l'invention a également

pour objet un système de distribution d'objets dans lequel les moyens d'acquisition de données du premier dispositif de communication correspondent à des instructions de produit programme d'ordinateur téléchargeable depuis un réseau de communication et/ou enregistré sur un support lisible par ordinateur et/ou exécutable par un processeur, lorsque le produit programme est exécuté sur ledit dispositif de communication.

BREVE DESCRIPTION DES FIGURES

[0028] D'autres caractéristiques et avantages de l'invention ressortiront à la lecture de la description qui suit, donnée uniquement à titre d'exemple, et faite en référence à :

- la figure 1 est une représentation schématique d'un système de distribution d'objets, le système comprenant deux dispositifs de communication et un équipement de réception d'objets, l'ensemble étant muni de six consignes et d'un dispositif de déverrouillage selon un mode de réalisation de l'invention, le dispositif de déverrouillage comprenant six serrures électroniques ;
- la figure 2 est une représentation schématique d'une des serrures électroniques de la figure 1, agencée au sein d'une des consignes ;
- la figure 3 est une représentation schématique d'une application stockée dans une mémoire d'un des dispositifs de communication de la figure 1 ;
- la figure 4 est une représentation schématique d'un dispositif de déverrouillage selon une variante de réalisation de l'invention.

DESCRIPTION DETAILLÉE D'UN MODE DE REALISATION

[0029] Dans la suite de la description, on entend par « ouvrant » tout élément mécanique mobile entre une position de fermeture d'un accès à une zone et une position d'ouverture permettant l'accès à la zone.

[0030] On entend également par « dispositif de communication » tout dispositif électronique nomade apte à transmettre et à recevoir des données via un réseau ou une portion de réseau sans fil, tel que par exemple un ordinateur portable, un téléphone, un smartphone, ou encore une tablette numérique, sans que cette liste ne soit exhaustive.

[0031] On entend en outre par « moyens moteurs » des moyens d'engagement mécanique permettant de faire évoluer une première position ou configuration mécanique d'un élément de l'invention vers une seconde position ou configuration mécanique.

[0032] On entend également par « consigne » tout contenant mécanique délimitant un espace intérieur pou-

vant recevoir un objet.

[0033] On appelle dans la suite de la description indifféremment une signature ou une clef numérique.

[0034] En référence à la figure 1, un système 1 de distribution d'objets comprend au moins un équipement 10 de réception d'objets, deux dispositifs de communication 12A, 12B et un ensemble 14 de stockage de données, relié à chaque dispositif de communication 12A, 12B via un réseau de communication 16. Dans l'exemple de réalisation de la figure 1, le système 1 de distribution d'objets comprend un seul équipement 10 de réception d'objets, un premier dispositif 12A de communication et un second dispositif 12B de communication. Dans cet exemple de réalisation particulier, le système 1 de distribution d'objets est relié, via le réseau de communication 16, à une base de données 17 de destinataires.

[0035] Le réseau de communication 16 est muni d'une infrastructure de communication privée ou étendue permettant la connexion, ou l'accès, à des équipements de communication de type serveurs et/ou bases de données et/ou appareils de communication mobiles. De manière classique, l'infrastructure de communication forme un réseau sans fil, ou un réseau filaire, ou encore un réseau comprenant une portion sans fil et une portion filaire. Dans un mode de réalisation particulier, le réseau de communication 16 est conçu comme comprenant une portion de réseau de type internet et une portion de réseau mobile de type UMTS (de l'anglais Universal Mobile Telecommunications System).

[0036] L'équipement 10 de réception d'objets comprend au moins une consigne 18 munie d'un ouvrant 20 formant accès à un espace intérieur de la consigne 18 destiné à recevoir un objet. L'équipement 10 comprend en outre un dispositif 22 de déverrouillage de l'ouvrant 20. Dans un mode de réalisation de l'invention illustré sur la figure 1, l'équipement 10 comporte au moins deux consignes 18. A titre d'exemple non limitatif, l'équipement 10 de réception d'objets comporte par exemple six consignes 18, comme représenté sur la figure 1.

[0037] Le dispositif de déverrouillage 22 comprend au moins une serrure électronique 24 et un module de commande 26 relié à la ou chaque serrure électronique 24 via une liaison de données 28. Dans le mode de réalisation de l'invention illustré sur la figure 1, le dispositif de déverrouillage 22 comprend au moins deux serrures électroniques 24. A titre d'exemple non limitatif, l'équipement 10 de réception d'objets comporte par exemple six serrures électroniques 24, comme représenté sur la figure 1. Chaque serrure électronique 24 est agencée au sein d'une des consignes 18 et est apte à verrouiller et déverrouiller l'ouvrant 20 de cette consigne 18. Le module de commande 26 est relié à chaque serrure électronique 24 via une liaison de données 28 distincte, trois liaisons de données 28 seulement étant représentées sur la figure 1 pour des raisons de clarté.

[0038] Chaque serrure électronique 24 comprend des moyens moteurs 30 et des moyens 32 de détection d'une fermeture de l'ouvrant 20 de la consigne 18 associée,

comme représenté sur la figure 2. Dans l'exemple de réalisation de l'invention des figures 1 et 2, chaque serrure électronique 24 comprend en outre des moyens 34 d'alimentation électrique des moyens moteurs 30.

[0039] Les moyens moteurs 30 sont aptes à verrouiller et déverrouiller l'ouvrant 20 suivant la valeur d'une consigne reçue via la liaison de données 28, comme détaillé par la suite. Les moyens moteurs 30 sont par exemple formés d'un micro-moteur permettant de faire mouvoir en translation un mécanisme protégeant la serrure contre des chocs liés au déplacement de l'ouvrant 20.

[0040] Les moyens de détection 32 sont aptes à émettre un signal de détection de la fermeture de l'ouvrant 20, sur la liaison de données 28. Dans l'exemple de réalisation de la figure 2, les moyens de détection 32 comprennent un capteur de mouvement 36 apte à détecter une fermeture de l'ouvrant 20 et un émetteur-récepteur de données 38 relié au capteur de mouvement 36 et à la liaison de données 28. L'émetteur-récepteur 38 est connecté en outre aux moyens moteurs 30.

[0041] Les moyens d'alimentation électrique 34 sont reliés aux moyens moteurs 30. Dans un mode de réalisation particulier, illustré sur la figure 2, les moyens d'alimentation électrique 34 comprennent une dynamo 40 munie d'un système piézo-électrique relié à l'ouvrant 20, ainsi qu'un élément de stockage d'énergie électrique 42 relié à la dynamo 40. Une telle configuration permet de générer un courant électrique lors de chaque mouvement d'ouverture et de fermeture de l'ouvrant 20 et de pouvoir ainsi recharger avantageusement l'élément de stockage d'énergie électrique 42, pour l'alimentation électrique des moyens moteurs 30.

[0042] En variante, les moyens d'alimentation électrique 34 comprennent un élément de stockage d'énergie électrique tel que des piles consommables, des piles rechargeables par un dispositif extérieur, ou encore une batterie. Selon cette variante, les moyens d'alimentation électrique 34 sont propres à générer un signal indicatif du niveau de charge courant des piles ou de la batterie, et l'émetteur-récepteur 38 est propre à transmettre ce signal au module de commande 26, via la liaison de données 28. Le module de commande 26 est alors propre à transmettre ce signal indicatif à l'ensemble de stockage 14, par exemple via un des dispositifs de communication 12A, 12B. Ceci permet notamment de générer une alerte destinée à informer qu'un remplacement ou une recharge de l'élément de stockage d'énergie électrique est nécessaire.

[0043] Le module de commande 26 comprend un capteur 44 de signaux, un composant électronique 46 relié au capteur 44 et à chaque liaison de données 28 et des moyens d'alimentation électrique 48 reliés au composant électronique 46, comme représenté sur la figure 1. Le module de commande 26 comprend en outre des moyens 50 d'émission de signaux et des moyens 52 de génération de clefs numériques reliés aux moyens d'alimentation électrique 48, au composant électronique 46 et aux moyens d'émission 50. De préférence, comme

illustré sur la figure 1, le module de commande 26 comprend également un composant 54 de codage de données.

[0044] Le capteur 44 est propre à recevoir un signal 56 comprenant une clef numérique CN, CNC émis par un dispositif 12A, 12B disposé à proximité du module de commande 26. Le capteur 44 est apte à transmettre ce signal 56 au composant électronique 46. Le capteur 44 est propre en outre à recevoir un signal de commande de verrouillage d'un des ouvrants 20 et à transmettre ce signal au composant électronique 46.

[0045] Le composant électronique 46 est un composant électronique de reconnaissance permettant d'authentifier une clef numérique CN reçue via le signal 56. Le composant électronique 46 est propre, lorsqu'il authentifie la clef numérique reçue CN, à générer un signal de consigne de désactivation d'un des moyens moteurs 30 pour le déverrouillage d'un des ouvrants 20, et à émettre ce signal sur la liaison de données 28 correspondante. Le composant électronique 46 est également propre, suite à la réception d'un signal de commande de verrouillage d'un des ouvrants 20, à générer un signal de consigne d'activation des moyens moteurs 30 pour le verrouillage de cet ouvrant 20, et à émettre ce signal sur la liaison de données 28 correspondante.

[0046] Le composant électronique 46 est par exemple muni d'un convertisseur analogique-numérique relié au capteur 44, et d'un module de calcul relié au convertisseur et formé d'au moins un processeur associé à au moins une mémoire, ces différents éléments n'étant pas représentés sur les figures pour des raisons de clarté.

[0047] De préférence, comme illustré sur la figure 1, le composant électronique 46 comprend également une horloge électronique 60. L'horloge électronique 60 est par exemple connectée au processeur du composant électronique 46.

[0048] Dans un mode de réalisation particulier, les moyens d'alimentation électrique 48 comprennent un élément de stockage d'énergie électrique et un élément de conversion d'énergie relié à l'élément de stockage d'énergie électrique. L'élément de conversion d'énergie est par exemple un élément de conversion d'une énergie lumineuse en énergie électrique tel que par exemple une cellule photovoltaïque. En variante, l'élément de conversion d'énergie est un élément de conversion d'une énergie thermique en énergie électrique. Ceci permet une recharge continue et autonome de l'élément de stockage d'énergie, et contribue ainsi à réduire voire à éliminer les opérations de remplacement des moyens d'alimentation électrique 48. Dans un autre mode de réalisation, les moyens d'alimentation électrique 48 sont formés par un élément de stockage d'énergie électrique tel que des piles consommables, des piles rechargeables par un dispositif extérieur, ou encore une batterie.

[0049] Les moyens d'émission 50 comprennent par exemple un émetteur radio-fréquences associé à un convertisseur numérique-analogique. L'émetteur radio-fréquences est par exemple propre à émettre un signal com-

pris dans le groupe consistant en : un signal de fréquence comprise dans la bande Bluetooth, un signal de fréquence comprise dans la bande NFC (Near Field Technology), un signal de fréquence comprise dans la bande Wi-Fi et un signal de fréquence comprise dans la bande Zigbee.

[0050] Les moyens 52 de génération de clefs numériques sont propres à générer une clef numérique unique à chaque fermeture d'un des ouvrants 20, les moyens d'émission 50 étant propres à émettre un signal 62 comportant la clef numérique générée. Plus précisément, les moyens de génération 52 sont propres à générer une clef numérique unique suite à chaque réception par le composant électronique 46 d'un signal de détection de la fermeture d'un des ouvrants 20. Les moyens de génération 52 sont également propres à transmettre chaque clef numérique générée au composant électronique 46, pour stockage dans sa mémoire, permettant ainsi une authentification ultérieure d'une clef numérique CN reçue par comparaison avec la clef numérique générée. Plus précisément, le composant électronique 46 n'est propre, pour chaque consigne 18, à authentifier une clef numérique CN reçue que par comparaison avec la dernière clef numérique générée lors de la fermeture de l'ouvrant 20 de cette consigne 18. Conformément à l'invention, le processeur du composant électronique 46 est propre, pour chaque consigne 18, à remplacer dans la mémoire du composant électronique 46 une éventuelle clef numérique déjà stockée par la clef numérique unique nouvellement générée lors de la fermeture de l'ouvrant 20 de la consigne 18. Ceci permet de réduire avantageusement l'espace mémoire nécessaire pour le stockage des clefs numériques dans la mémoire du composant électronique 46.

[0051] Les moyens de génération 52 sont par exemple formés d'un module logiciel de génération de clefs numériques uniques.

[0052] Dans l'exemple de réalisation préférentiel selon lequel le composant électronique 46 comprend également une horloge électronique 60, une information d'horodatage est associée à la clef numérique unique générée et le composant électronique 46 n'est propre à authentifier une clef numérique CN reçue par comparaison avec la clef numérique générée que pendant une durée prédéterminée. Ceci permet, en cas de vol d'une clef numérique unique après son émission par le module de commande 26, de réduire la durée d'une fenêtre temporelle « fictive » durant laquelle l'accès à l'espace intérieur d'une consigne 18 peut être compromis. Un gain de sécurité supplémentaire est ainsi obtenu.

[0053] Le composant 54 de codage de données est connecté d'une part entre le capteur 44 et le composant électronique 46, et d'autre part entre les moyens 52 de génération de clefs numériques et les moyens 50 d'émission de signaux. Le composant de codage 54 est propre à coder les clefs numériques uniques générées par les moyens de génération 52. Le composant de codage 54 est propre en outre à décoder une clef numérique codée

CNC contenue dans le signal 56 et à transmettre la clef numérique décodée CN au composant électronique 46. Le composant de codage 54 est propre également à transmettre les clefs numériques codées aux moyens d'émission 50, après réception par le composant électronique 46 d'un signal de commande de verrouillage d'un des ouvrants 20. Les moyens moteurs 30 de chaque serrure électronique 24 sont aptes à verrouiller l'ouvrant 20 associé lors de la fermeture de l'ouvrant 20. Selon une variante, le composant de codage 54 est propre à transmettre les clefs numériques codées aux moyens d'émission 50 sitôt après leur codage.

[0054] Dans l'exemple de réalisation préférentiel de la figure 1, le composant de codage 54 est un composant de chiffrement symétrique. Plus particulièrement, le composant de codage 54 est propre à appliquer, sur la clef numérique unique générée par les moyens de génération 52, un algorithme de chiffrement symétrique ayant pour paramètre une clef cryptographique symétrique. Dans un mode de réalisation préférentiel, le composant de chiffrement symétrique 54 comporte une mémoire. Selon ce mode de réalisation préférentiel, le composant de chiffrement symétrique 54 est propre à régénérer, au bout d'une durée prédéterminée, une nouvelle clef cryptographique symétrique servant de paramètre à l'algorithme de chiffrement symétrique, et à conserver dans sa mémoire la ou chaque clef cryptographique symétrique générée précédemment, tant que des clefs numériques uniques codées par ces clefs symétriques sont encore en circulation. Ceci permet, en cas de vol d'une clef de chiffrement symétrique après sa génération par le composant de chiffrement symétrique 54, de réduire la durée d'une fenêtre temporelle « fictive » durant laquelle l'accès à l'espace intérieur d'une consigne 18 peut être compromis. Un gain de sécurité supplémentaire est ainsi obtenu.

[0055] En conservant la clef cryptographique symétrique générée, le composant de codage 54 est ainsi le seul à pouvoir décoder les clefs numériques codées transmises aux moyens d'émission 50. Ceci permet d'augmenter le niveau de confidentialité des clefs générées. Dans une variante de réalisation, le composant de codage 54 est un composant de masquage ou d'obfuscation de données. Dans un autre mode de réalisation, qui peut se combiner aux modes de réalisation précédents, le composant de codage 54 est propre en outre à appliquer, sur une clef numérique qu'il a préalablement codée, un algorithme de chiffrement asymétrique ayant pour paramètre une clef cryptographique publique préalablement transmise par l'ensemble de stockage 14. L'algorithme de chiffrement asymétrique est par exemple un algorithme de type RSA (Rivest Shamir Adleman). Ceci permet d'éviter, en cas de compromission du composant de codage 54 par un utilisateur mal intentionnée, que cet utilisateur puisse compromettre l'accès à l'ensemble des consignes 18. Un gain de sécurité supplémentaire est ainsi obtenu. Dans un autre mode de réalisation, qui peut se combiner aux modes de réalisation précédents, le

composant de codage 54 est propre à adjoindre une signature numérique à chaque clef numérique unique générée. La signature numérique est par exemple une signature numérique de type SHA (Secure Hash Algorithm).

[0056] Chaque liaison de données 28 est une liaison bidirectionnelle filaire ou non filaire. Dans le mode de réalisation de l'invention de la figure 1, chaque liaison de données 28 est par exemple une liaison point à point codée bidirectionnelle.

[0057] Chaque dispositif de communication 12A, 12B est propre à émettre un signal 56 comprenant une clef numérique codée CNC ou non codée CN. Plus précisément, chaque dispositif de communication 12A, 12B comprend un émetteur 64 apte à émettre un tel signal 56 sur une liaison sans fil 65. Chaque dispositif de communication 12A, 12B comprend en outre des moyens 66 de réception de données transportées sur la liaison sans fil 65, tels qu'un récepteur de signal comme illustré sur la figure 1. De préférence, comme représenté sur cette figure, chaque dispositif de communication 12A, 12B est muni également d'une unité de calcul formée d'un processeur 70 relié à une mémoire 72, et de moyens 74 d'acquisition de données.

[0058] L'émetteur 64 est par exemple un émetteur radio-fréquences propre à émettre un signal compris dans le groupe consistant en : un signal de fréquence comprise dans la bande Bluetooth, un signal de fréquence comprise dans la bande NFC (Near Field Technology), un signal de fréquence comprise dans la bande Wi-Fi et un signal de fréquence comprise dans la bande Zigbee. L'émetteur 64 est relié en outre au réseau de communication 16 et est propre également à émettre des signaux radioélectriques conformes à la norme UMTS.

[0059] Chaque liaison sans fil 65 est par exemple une liaison sans fil choisie dans le groupe consistant en : une liaison Bluetooth, une liaison NFC, une liaison Wi-Fi et une liaison Zigbee.

[0060] Les moyens 66 de réception de données sont propres à communiquer avec les moyens d'émission 50 du dispositif de déverrouillage 22 de sorte à recevoir chaque clef numérique unique générée par le dispositif 22. L'émetteur 64 est propre à transmettre chaque clef numérique unique reçue à l'ensemble de stockage 14, via le réseau de communication 16.

[0061] Les moyens de réception 66 sont reliés en outre au réseau de communication 16 et sont propres également à recevoir des signaux radioélectriques conformes à la norme UMTS.

[0062] Le processeur 70 est connecté à l'émetteur 64, aux moyens 66 de réception de données et aux moyens 74 d'acquisition de données. Dans un mode de réalisation particulier, le processeur 70 est propre à générer, suite à la réception d'un signal de commande transmis par les moyens 74 d'acquisition de données, un signal indicatif de l'état « libre » d'une des consignes 18. Le processeur 70 est propre à transmettre ce signal à l'émetteur 64, pour transmission à l'ensemble de stockage 14.

Le processeur 70 est également propre à générer, suite à la réception d'un signal de commande transmis par les moyens 74 d'acquisition de données, un signal de commande de verrouillage d'un des ouvrants 20 et à transmettre ce signal à l'émetteur 64, pour émission sur la liaison sans fil 65.

[0063] Dans un mode de réalisation particulier, la mémoire 72 est apte à stocker chaque clef numérique unique générée par le dispositif de déverrouillage 22. Selon ce mode de réalisation, le processeur 70 est propre à commander la transmission à l'ensemble de stockage 14, via l'émetteur 64, de chaque clef numérique stockée dans la mémoire 72 uniquement si la connexion est établie sur le réseau 16 entre le dispositif de communication 12A, 12B et l'ensemble de stockage 14. Ceci permet d'assurer une transmission à l'ensemble de stockage 14 de toutes les clefs numériques uniques générées par le dispositif de déverrouillage 22, et ce même si au moment de leur réception par le dispositif de communication 12A, 12B la connexion n'est pas possible sur le réseau 16. Ainsi, la mise en oeuvre du système de distribution d'objets 1 est facilitée, quelle que soit la couverture du réseau de communication 16 relativement à la localisation de l'équipement de réception d'objets 10.

[0064] Les moyens 74 d'acquisition de données comprennent une interface utilisateur 76 et une application 78A, 78B stockée au sein de la mémoire 72 et propre à être mise en oeuvre par le processeur 70. Plus précisément, les moyens 74 d'acquisition de données du premier dispositif de communication 12A, respectivement du deuxième dispositif de communication 12B, comprennent une première application 78A, respectivement une deuxième application 78B.

[0065] L'interface utilisateur 76 du premier dispositif de communication 12A est par exemple un écran tactile. L'interface utilisateur 76 du deuxième dispositif de communication 12B comprend par exemple un écran tactile associé à un capteur de données de géolocalisation de type GPS (Global Positioning System) et/ou à un appareil photographique.

[0066] La première application 78A est par exemple téléchargeable depuis le réseau de communication 16. La première application 78A comprend un module d'acquisition d'une entrée d'identification d'un utilisateur. Une telle entrée d'identification peut par exemple prendre la forme d'une suite de caractères alpha-numériques, une telle suite de caractères alpha-numériques pouvant par exemple correspondre à une identité numérique de type Identité Numérique Vérifiée d'un utilisateur, comme détaillé par la suite. Avantagusement, la première application 78A inclue également un module de signature électronique.

[0067] La deuxième application 78B est par exemple téléchargeable depuis le réseau de communication 16. Dans un mode de réalisation particulier, la deuxième application 78B comprend un module 80 d'acquisition de données et/ou un module 82 de contrôle de conformité d'une identité d'un utilisateur et/ou un module 84 de créa-

tion d'une identité numérique et/ou un module 86 de signature électronique. Dans l'exemple de réalisation illustratif de la figure 3, la deuxième application 78B comprend les quatre modules 80, 82, 84, 86 précités.

[0068] Le module 80 d'acquisition de données est par exemple propre, en combinaison avec l'interface utilisateur 76, à acquérir des données d'entrée sous forme de données textuelles, de données de géolocalisation ou encore de photographies. Un utilisateur du deuxième dispositif de communication 12B, porteur d'un ou plusieurs objets à distribuer via le système 1 de distribution d'objets, peut ainsi avantageusement enregistrer dans le deuxième dispositif de communication 12B l'adresse d'un utilisateur destinataire, ou encore une entrée d'identification correspondant à une identité numérique de l'utilisateur, ou bien acquérir une photographie d'une pièce d'identité de l'utilisateur.

[0069] Le module 82 de contrôle de conformité d'une identité d'un utilisateur est propre, à partir d'une identité numérique ou d'une photographie d'une pièce d'identité acquises par le module d'acquisition 80, à comparer cette identité numérique ou cette photographie à une liste pré-enregistrée d'identités ou de pièces d'identité considérées comme « valides ». La liste pré-enregistrée est par exemple stockée dans la mémoire 72. En variante, la liste pré-enregistrée est stockée dans un serveur distant relié au deuxième dispositif de communication 12B via le réseau de communication 16. En fonction du résultat de la comparaison effectuée, le module de contrôle de conformité 82 est ainsi propre à authentifier l'identité d'un utilisateur, par exemple un utilisateur destinataire d'un objet ou document.

[0070] Dans un exemple de réalisation particulier, le module 84 de création d'une identité numérique est propre à créer une identité numérique de type Identité Numérique Vérifiée, appelée dans la suite de la description « IDN ».

[0071] L'IDN est ici présentée en combinaison avec la présente invention, mais il est à noter que le processus de délivrance de l'IDN ainsi que toutes les caractéristiques afférentes, peuvent être mises en oeuvre de manière indépendante de la présente invention et de ses modes de réalisation. Ainsi, le système IDN tel que décrit par la suite permet à un utilisateur IDN de disposer d'une identité numérique vérifiée, qui peut être utilisée à des fins d'identification pour tout type de services.

[0072] Le système IDN va maintenant être décrit de manière indépendante.

[0073] Dans un système IDN, les attributs d'un utilisateur IDN concernent, notamment :

- des informations de compte (pseudonyme, mot de passe),
- l'identité de l'utilisateur IDN (civilité, nom, prénom, date de naissance),
- une adresse physique, postale ou géographique

(nom rue, code postal, ville, pays, ...),

- un identifiant numérique d'un document d'identité de l'utilisateur,
- une adresse électronique,
- un numéro de téléphone mobile.

[0074] Le principe du système IDN est qu'un utilisateur IDN déclare des informations, qui seront vérifiées par le module de contrôle de conformité 82, et qui pourront ensuite être utilisées sans nécessiter une nouvelle vérification à chaque utilisation.

[0075] La mise en oeuvre d'un processus IDN comprend, par exemple, les étapes suivantes :

1. Une étape de début de l'inscription au cours de laquelle un utilisateur IDN déclare, par exemple via l'interface utilisateur 76, des éléments de son identité (civilité, nom, prénom, date de naissance, adresse e-mail, adresse postale, numéro de téléphone mobile) et d'un mot de passe personnel ;

2. Une d'étape au cours de laquelle le service IDN envoie un message de notification d'inscription à l'adresse électronique déclarée par l'utilisateur IDN ; ce message contient, notamment, un lien url vers une page permettant de confirmer l'inscription et de ce fait l'identifiant IDN de l'utilisateur du service IDN ;

3. Une étape au cours de laquelle l'utilisateur IDN confirme l'inscription, par exemple en se rendant sur un site web correspondant au lien fourni dans le message ;

4. Une étape au cours de laquelle le service envoie un code d'activation par SMS au numéro de téléphone mobile déclaré par l'utilisateur IDN ;

5. Une étape au cours de laquelle l'utilisateur IDN saisit, via l'interface, le code SMS reçu, afin que l'existence et la validité du numéro de mobile qu'il a déclaré soient vérifiées et confirmées ;

6. Une étape au cours de laquelle le service envoie, à l'utilisateur IDN, un code d'activation par courrier postal à l'adresse qu'il a déclarée ;

7. Une étape au cours de laquelle le courrier postal, ou tout moyen de délivrance du code d'activation, est remis au domicile, en mains propres ou par tout autre moyen permettant de vérifier l'adresse postale du destinataire ainsi que l'identité de l'utilisateur du service IDN ;

8. Une étape au cours de laquelle l'utilisateur IDN saisit, par exemple via l'interface utilisateur 76, le

code d'activation reçu par courrier et remis en mains propres, ceci afin de valider l'adresse physique déclarée par l'utilisateur IDN et de confirmer la vérification de l'identité de l'utilisateur IDN qu'il a déclarée ;

9. Une étape finale au cours de laquelle le service confirme à l'utilisateur IDN, via le module 84 de création d'une identité numérique, la création de son IDN personnel.

[0076] Ainsi, un tel service IDN permet de vérifier une à une l'ensemble, ou un sous-ensemble, des données fournies par l'utilisateur IDN et notamment l'identité qu'il a déclarée. Les données de l'utilisateur sont stockées de manière sécurisée.

[0077] L'ensemble 14 de stockage de données est relié à la base de données 17 de destinataires, via le réseau de communication 16. L'ensemble de stockage 14 est relié en outre au ou à chaque équipement 10 de réception d'objets, via le réseau de communication 16. Dans l'exemple de réalisation de la figure 1, l'ensemble de stockage 14 est relié à l'équipement 10 de réception d'objets via le réseau de communication 16 et les dispositifs de communication 12A, 12B. En variante non représentée, l'ensemble de stockage 14 est relié directement à l'équipement 10 via le réseau de communication 16 qui est par exemple un réseau de communication bas débit, et le module de commande 26 du dispositif de déverrouillage 22 comprend un terminal d'accès au réseau de communication 16.

[0078] L'ensemble 14 de stockage de données est propre à stocker chaque clef numérique unique générée par le dispositif de déverrouillage 22. Dans l'exemple de réalisation de la figure 1, l'ensemble de stockage 14 comprend un serveur 88 relié à une base de données 90.

[0079] Le serveur 88 comprend par exemple un processeur 92 et une mémoire 94 reliée au processeur 92.

[0080] Le processeur 92 est propre à transmettre, au premier dispositif de communication 12A, chaque clef numérique unique fournie par le deuxième dispositif de communication 12B. Le processeur 92 est propre à générer des messages de notification. Le processeur 92 est ainsi propre à transmettre au premier dispositif de communication 12A, pour chaque clef numérique reçue du deuxième dispositif de communication 12B, un message de notification indicatif de la présence d'un objet dans une des consignes 18.

[0081] Selon un mode de réalisation particulier de l'invention, la mémoire 94 forme un module de gestion de la disponibilité des consignes 18. Selon ce mode de réalisation, le module de gestion 94 comprend une table 96 de stockage de plusieurs bulletins de consignations. Chaque bulletin de consignation est associé à une des consignes 18 et est apte à prendre une première valeur correspondant à un état « libre » de la consigne 18, et une deuxième valeur correspondant à un état « occupé » de la consigne 18. Le processeur 92 est propre à modi-

fier, dans la table de stockage 96, la valeur courante de chaque bulletin de consignation. Ceci permet de pouvoir affecter séquentiellement une même consigne 18 à différents utilisateurs, sans risque quant à la confidentialité des objets déposés. En particulier, le processeur 92 est propre, suite à la réception d'un signal indicatif de l'état « libre » d'une des consignes 18, à affecter la première valeur correspondant à l'état « libre » au bulletin de consignation associé à cette consigne 18.

[0082] La base de données 90 est propre à stocker chaque clef numérique unique générée par le dispositif de déverrouillage 22. Dans l'exemple de réalisation de la figure 1, la base de données 90 est propre à stocker chaque clef numérique unique transmise par le deuxième dispositif de communication 12B. De préférence, la base de données 90 est également propre à stocker une table associant des identifiants de dispositifs de communication 12A, 12B à des données d'identification de destinataires pré-enregistrés.

[0083] La base de données 17 de destinataires stocke des enregistrements préalablement validés comme des valeurs d'authentification de destinataires, par exemple obtenus suite à la mise en oeuvre d'un processus IDN tel que décrit ci-dessus. Dans l'exemple de réalisation particulier de la figure 1, le processeur 92 est propre à transmettre, au premier dispositif de communication 12A, chaque clef numérique unique reçue uniquement si une entrée d'identification acquise via les moyens 74 d'acquisition de données du premier dispositif de communication 12A correspond à un des enregistrements de la base de données 17 de destinataires.

[0084] Le fonctionnement du système 1 de distribution d'objets va maintenant être décrit.

[0085] On suppose que l'utilisateur du deuxième dispositif de communication 12B, appelé ci-après « distributeur », est porteur d'un objet à distribuer à destination de l'utilisateur du premier dispositif de communication 12A appelé ci-après « destinataire ». L'objet à distribuer est par exemple une lettre recommandée munie d'un code numérique d'identification de la lettre. On suppose qu'initialement une des consignes 18 est libre, c'est-à-dire que le bulletin de consignation associé à cette consigne dans le module de gestion 94 présente la première valeur correspondant à l'état « libre ». On suppose que l'ouvrant 20 de cette consigne 18 est verrouillé et que les autres consignes 18 sont occupées. On suppose enfin que la base de données 90 stocke une clef numérique codée CNC apte, après décodage, à être authentifiée par le composant électronique 46 pour le déverrouillage de l'ouvrant 20. La mémoire du composant électronique 46 stocke une clef numérique d'authentification initiale.

[0086] Le distributeur commence par scanner, via son dispositif de communication 12B, le code numérique de la lettre recommandée. Ce code numérique est alors enregistré par le module d'acquisition de données 80 puis transmis à l'ensemble de stockage 14.

[0087] Au cours d'une étape suivante, le distributeur

saisit, dans l'interface utilisateur 76 du deuxième dispositif de communication 12B, une entrée d'identification correspondant à une identité numérique du destinataire. Une fois acquise par le module 80, cette entrée d'identification est transmise à l'ensemble de stockage 14 via l'émetteur 64.

[0088] Le processeur 92 de l'ensemble de stockage 14 vérifie alors que l'entrée d'identification reçue correspond à un des enregistrements stockés dans la base de données 17. Si cette vérification est positive, le processeur 92 consulte les bulletins de consignation stockés dans la table 96 et vérifie leur valeur courante afin d'identifier une éventuelle consigne 18 libre. Sinon, le processeur 92 en informe le deuxième dispositif de communication 12B et le procédé s'arrête. Si le processeur 92 identifie une consigne 18 libre, il réserve cette consigne 18, c'est-à-dire qu'il affecte la deuxième valeur correspondant à l'état « occupé » au bulletin de consignation associé à cette consigne 18. Sinon, le processeur 92 en informe le deuxième dispositif de communication 12B et le procédé s'arrête. Dans l'exemple de réalisation décrit ici, le processeur 92 identifie le seul bulletin de consignation présentant la première valeur correspondant à l'état « libre » et affecte la deuxième valeur correspondant à l'état « occupé » à ce bulletin de consignation.

[0089] Au cours d'une étape suivante, le processeur 92 récupère la clef numérique codée CNC stockée dans la base de données 90 et transmet, au deuxième dispositif de communication 12B, cette clef numérique codée CNC accompagnée d'un identifiant de la consigne 18 réservée.

[0090] Au cours d'une étape suivante, le distributeur, muni du deuxième dispositif de communication 12B, s'approche du module de commande 26 et saisit, dans l'interface utilisateur 76 du dispositif 12B, une instruction d'envoi de la clef numérique codée CNC au module de commande 26. Le deuxième dispositif de communication 12B émet alors le signal 56 contenant la clef numérique codée CNC sur la liaison sans fil 65, à destination du module de commande 26. Après réception par le capteur 44, la clef numérique codée CNC est décodée par le composant de codage 54 puis transmise au composant électronique de reconnaissance 46. Le composant électronique de reconnaissance 46 authentifie la clef numérique CN, génère un signal de consigne de désactivation des moyens moteurs 30 de la serrure électronique 24 concernée, et émet ce signal sur la liaison de données 28 associée. Après réception par la serrure électronique 24 du signal de consigne de désactivation des moyens moteurs, les moyens moteurs 30 déverrouillent l'ouvrant 20, libérant ainsi l'accès à l'espace intérieur de la consigne 18.

[0091] Au cours d'une étape suivante, le distributeur consulte sur son dispositif de communication 12B l'identifiant de la consigne 18 réservée, s'approche de cette consigne 18 et ouvre l'ouvrant 20 de la consigne 18. En variante, le déverrouillage de l'ouvrant 20 par les moyens moteurs 30 ouvre automatiquement l'ouvrant 20, four-

nissant ainsi une information visuelle permettant au distributeur d'identifier la consigne 18 réservée. Le distributeur place alors l'objet à distribuer, en l'espèce la lettre recommandée, dans l'espace intérieur de la consigne 18 et referme l'ouvrant 20 de la consigne.

[0092] Au cours d'une étape suivante, les moyens de détection 32 agencés dans la consigne 18 détectent la fermeture de l'ouvrant 20 et émettent un signal de détection de la fermeture de l'ouvrant 20 sur la liaison de données 28. Suite à la réception du signal de détection par le composant électronique de reconnaissance 46, les moyens de génération 52 génèrent une clef numérique unique. Les moyens de génération 52 transmettent cette clef numérique unique au composant électronique 46 et au composant de codage 54. Le composant électronique 46 remplace la clef numérique d'authentification initiale par la nouvelle clef numérique unique dans sa mémoire, et le composant de codage 54 code la clef numérique.

[0093] Au cours d'une étape suivante, le distributeur saisit, via l'interface utilisateur 76 du dispositif 12B, une instruction de commande de verrouillage de l'ouvrant 20. Le processeur 70 génère alors le signal de commande de verrouillage de l'ouvrant 20, et transmet ce signal à l'émetteur 64, pour émission sur la liaison sans fil 65. Suite à la réception du signal de commande par le composant électronique 46 via le capteur 44, le composant électronique 46 génère un signal de consigne d'activation des moyens moteurs 30 pour le verrouillage de l'ouvrant 20, et émet ce signal sur la liaison de données 28 associée. Après réception par la serrure électronique 24 du signal de consigne de d'activation des moyens moteurs, les moyens moteurs 30 verrouillent l'ouvrant 20. A l'issue de cette étape, le composant de codage 54 transmet la clef numérique codée aux moyens d'émission 50 du module de commande 26. Les moyens d'émission 50 transmettent le signal 62 comportant la clef numérique codée au deuxième dispositif de communication 12B, via la liaison sans fil 65.

[0094] Au cours d'une étape suivante, si la connexion est établie sur le réseau 16 entre le deuxième dispositif de communication 12B et l'ensemble de stockage 14, le processeur 70 commande la transmission à l'ensemble de stockage 14, via l'émetteur 64, de la clef numérique unique codée. Dans un mode de réalisation particulier, si la connexion n'est pas établie sur le réseau 16 entre le deuxième dispositif de communication 12B et l'ensemble de stockage 14, la mémoire 72 stocke la clef numérique unique codée. Le processeur 70 commande alors, au cours d'une étape suivante, la transmission à l'ensemble de stockage 14 de la clef numérique stockée dans la mémoire 72 dès que la connexion est établie sur le réseau 16.

[0095] Au cours d'une étape suivante, le serveur 88 reçoit la clef numérique unique codée. Le processeur 92 du serveur 88 associe la clef numérique unique codée à l'entrée d'identification du destinataire préalablement reçue, et commande le stockage de ces données dans la

base de données 90. La clef numérique unique ainsi stockée est une clef numérique codée CNC.

[0096] Au cours d'une étape suivante, le processeur 92 identifie, via la table stockée dans la base de données 90, le premier dispositif de communication 12A comme étant le dispositif de communication du destinataire. Le processeur 92 génère alors un message de notification indicatif de la présence de la lettre recommandée dans une des consignes 18 et transmet ce message au premier dispositif de communication 12A. Selon un exemple de réalisation préférentiel, le destinataire recevant le message de notification saisit dans l'interface utilisateur 76 du dispositif 12A une entrée d'identification, par exemple une identité numérique de type Identité Numérique Vérifiée. Le dispositif de communication 12A transmet l'entrée d'identification saisie au serveur 88, et le processeur 92 du serveur 88 vérifie si l'entrée d'identification saisie correspond à un des enregistrements de la base de données 17 de destinataires. Si la vérification est positive, le processeur 92 transmet au premier dispositif de communication 12A la clef numérique unique codée CNC, stockée dans la base de données 90. Sinon, cela signifie que l'utilisateur du premier dispositif de communication 12A n'est pas le destinataire prévu, et la clef numérique unique codée CNC n'est pas transmise au premier dispositif de communication 12A. Ceci permet d'obtenir une authentification plus sûre de l'identité du destinataire, préalablement à la remise de la clef numérique à ce destinataire. Dans un autre exemple de réalisation, la clef numérique unique codée CNC est transmise par le processeur 92 conjointement au message de notification.

[0097] Dans l'exemple de réalisation particulier décrit, le destinataire signe ensuite « électroniquement », via son interface utilisateur 76 et le module de signature électronique de la première application 78A de son dispositif 12A, la lettre recommandée reçue. Cette caractéristique permet une application avantageuse du système de distribution d'objets selon l'invention à la réception d'objets remis contre une signature, tels qu'une lettre recommandée par exemple. En effet, aucune présence physique du destinataire de l'objet remis contre signature n'est nécessaire lors de la réception de l'objet.

[0098] Au cours d'une étape suivante, le destinataire procède à la récupération de l'objet reçu dans une des consignes 18. Pour ce faire, une première possibilité est que le destinataire se rende à proximité du module de commande 26. Le destinataire saisit alors, dans l'interface utilisateur 76 du dispositif 12A, une instruction d'envoi de la clef numérique codée CNC au module de commande 26. Le premier dispositif de communication 12A émet alors le signal 56 contenant la clef numérique codée CNC sur la liaison sans fil 65, à destination du module de commande 26. Après réception par le capteur 44, la clef numérique codée CNC est décodée par le composant de codage 54 puis transmise au composant électronique de reconnaissance 46. Le composant électronique de reconnaissance 46 authentifie la clef numérique

CN, génère un signal de consigne de désactivation des moyens moteurs 30 de la serrure électronique 24 concernée, et émet ce signal sur la liaison de données 28 associée. Après réception par la serrure électronique 24 du signal de consigne de désactivation des moyens moteurs, les moyens moteurs 30 déverrouillent l'ouvrant 20, libérant ainsi l'accès à l'espace intérieur de la consigne 18.

[0099] Au cours d'une étape suivante, le destinataire consulte sur son dispositif de communication 12A l'identifiant de la consigne 18 renfermant l'objet, s'approche de cette consigne 18 et ouvre l'ouvrant 20 de la consigne 18. En variante, le déverrouillage de l'ouvrant 20 par les moyens moteurs 30 ouvre automatiquement l'ouvrant 20, fournissant ainsi une information visuelle permettant au destinataire d'identifier la consigne 18. Le destinataire récupère alors l'objet, en l'espèce la lettre recommandée, dans l'espace intérieur de la consigne 18 et referme l'ouvrant 20 de la consigne.

[0100] Au cours d'une étape suivante, les moyens de détection 32 agencés dans la consigne 18 détectent la fermeture de l'ouvrant 20 et émettent un signal de détection de la fermeture de l'ouvrant 20 sur la liaison de données 28. Suite à la réception du signal de détection par le composant électronique de reconnaissance 46, les moyens de génération 52 génèrent une clef numérique unique. Les moyens de génération 52 transmettent cette clef numérique unique au composant électronique 46 et au composant de codage 54. Le composant électronique 46 remplace, dans sa mémoire, la clef numérique d'authentification présente par la nouvelle clef numérique générée, et le composant de codage 54 code la clef numérique et transmet la clef numérique codée aux moyens d'émission 50. Les moyens d'émission 50 transmettent le signal 62 comportant la clef numérique codée au premier dispositif de communication 12A, via la liaison sans fil 65.

[0101] Au cours d'une étape suivante, si la connexion est établie sur le réseau 16 entre le premier dispositif de communication 12A et l'ensemble de stockage 14, le processeur 70 commande la transmission à l'ensemble de stockage 14, via l'émetteur 64, de la clef numérique unique codée. Dans un mode de réalisation particulier, si la connexion n'est pas établie sur le réseau 16 entre le premier dispositif de communication 12A et l'ensemble de stockage 14, la mémoire 72 stocke la clef numérique unique codée. Le processeur 70 commande alors, au cours d'une étape suivante, la transmission à l'ensemble de stockage 14 de la clef numérique stockée dans la mémoire 72 dès que la connexion est établie sur le réseau 16. La clef numérique unique ainsi stockée dans l'ensemble de stockage 14 est une clef numérique codée CNC.

[0102] Au cours d'une étape suivante, le destinataire saisit, via l'interface utilisateur 76 du dispositif 12A, une instruction de commande de « libération » de la réservation de la consigne 18. Suite à la réception de cette instruction de commande, le processeur 70 du dispositif 12A

génère un signal indicatif de l'état « libre » de la consigne 18 et transmet ce signal au serveur 88, via l'émetteur 64. Le processeur 92 du serveur 88 libère alors la réservation de la consigne 18, c'est-à-dire qu'il affecte la première valeur correspondant à l'état « libre » au bulletin de consignation associé à cette consigne 18.

[0103] En variante de la première possibilité décrite ci-avant, une deuxième possibilité est que le destinataire saisisse, dans l'interface utilisateur 76 du dispositif 12A, une instruction de transfert de la clef numérique codée CNC à un dispositif de communication d'un autre utilisateur, appelé par la suite « mandataire ». Selon cette variante, la base de données 90 est propre à stocker une liste de données d'identification de mandataires pré-enregistrés, ainsi qu'une table associant des identifiants de dispositifs de communication à ces données d'identification. Le premier dispositif 12A émet alors un signal de demande de transfert de la clef numérique codée CNC, à destination de l'ensemble de stockage 14. Suite à la réception de ce signal par le processeur 92, celui-ci vérifie, via la liste stockée dans la base de données 90, que le mandataire demandé est un des mandataires pré-enregistrés. Si la vérification est négative, un nouveau message de notification indicatif du caractère non autorisé du mandataire est transmis au premier dispositif de communication 12A. Si la vérification est positive, le processeur 92 identifie, via la table stockée dans la base de données 90, le dispositif de communication associé au mandataire demandé, puis génère un message de notification indicatif d'une demande de récupération de la lettre recommandée dans une des consignes 18, et transmet ce message au dispositif de communication du mandataire. Selon un exemple de réalisation préférentiel, le mandataire recevant le message de notification saisit dans l'interface utilisateur de son dispositif de communication une entrée d'identification, par exemple une identité numérique de type Identité Numérique Vérifiée. Le dispositif de communication transmet alors l'entrée d'identification saisie au serveur 88, et le processeur 92 du serveur 88 vérifie si l'entrée d'identification saisie correspond à un des enregistrements de la base de données 17. Si la vérification est positive, le processeur 92 transmet au dispositif de communication du mandataire la clef numérique unique codée CNC, stockée dans la base de données 90. Sinon, cela signifie que l'utilisateur du dispositif de communication n'est pas le mandataire prévu, et la clef numérique unique codée CNC n'est pas transmise à ce dernier. Les étapes suivantes de récupération de l'objet par le mandataire sont identiques aux étapes de récupération de l'objet par le destinataire exposées précédemment, et ne sont donc pas décrites plus en détail.

[0104] Cette variante de réalisation permet à un mandataire de récupérer l'objet à distribuer en cas d'absence du destinataire, et d'ainsi pouvoir avantageusement libérer la consigne 18 concernée pour une éventuelle autre utilisation. Ceci permet ainsi de réduire les coûts d'exploitation.

[0105] On conçoit ainsi que le dispositif de déverrouillage 22 selon l'invention permet d'assurer de manière simple et fiable la fermeture et le déverrouillage de l'ouvrant 20, tout en améliorant le niveau de sécurité du dispositif.

[0106] La figure 4 illustre une variante de réalisation de l'invention pour laquelle les éléments analogues au premier exemple de réalisation, décrit précédemment en regard des figures 1 à 3, sont repérés par des références identiques, et ne sont donc pas décrits à nouveau.

[0107] Dans cette variante de réalisation, le dispositif de déverrouillage 22 comprend autant de modules de commande 26 que de serrures électroniques 24, le nombre de modules de commande 26 étant en outre égal au nombre de consignes 18. Chaque module de commande 26 est en effet agencé au sein d'une des consignes 18 et est connecté à la serrure électronique 24 agencée au sein de cette consigne, via une des liaisons de données 28. Dans un exemple de réalisation particulier de cette variante, l'équipement 10 de réception d'objets comprend une seule consigne 18 munie d'un ouvrant 20, et le dispositif de déverrouillage 22 comprend une seule serrure électronique 24 et un seul module de commande 26, agencés au sein de la consigne 18.

[0108] Dans l'exemple de réalisation de la figure 4, les moyens d'alimentation électrique 34 comprennent un élément 42 de stockage d'énergie électrique tel que par exemple des piles consommables.

[0109] De préférence, selon cette variante de réalisation, chaque liaison de données 28 est une liaison filaire bidirectionnelle.

[0110] De préférence, selon cette variante de réalisation, l'émetteur 64 de chaque dispositif de communication 12A, 12B est un émetteur propre à émettre un signal sonore de fréquence comprise dans la bande audio [20 Hz - 16 kHz]. De manière alternative, l'émetteur est propre à émettre un signal de fréquence inférieure à 20 Hz ou encore un signal de fréquence supérieure à 16 kHz. Ceci permet par exemple d'utiliser en tant qu'émetteur 64 le haut-parleur de n'importe quel téléphone 12A, 12B classique et en tant que capteur 44 de signaux un capteur audio. Ceci permet en outre à une consigne 18 donnée de reconnaître automatiquement, lors de la réception du signal 56 comprenant une clef numérique codée CNC ou non codée CN, le dispositif de communication 12A, 12B émetteur du signal.

[0111] En fonctionnement, la seule différence entre le système de distribution d'objets selon la variante de réalisation illustrée sur la figure 4 et le système de distribution d'objets selon le premier mode de réalisation illustré sur les figures 1 à 3 est que le distributeur, comme le destinataire, au lieu de s'approcher d'un module de commande unique pour émettre une clef numérique codée CNC, s'approche de la consigne 18 concernée qui contient un des modules de commande.

[0112] Le reste du fonctionnement du système de distribution d'objets selon la variante de réalisation illustrée sur la figure 4 étant similaire à celui du système de dis-

tribution d'objets selon le premier mode de réalisation illustré sur les figures 1 à 3, celui-ci ne sera pas décrit plus en détail.

[0113] Le système de distribution d'objets selon l'invention offre plusieurs avantages :

- il permet à un utilisateur destinataire d'un objet, par exemple un objet remis contre signature, de pouvoir récupérer cet objet rapidement dans une des consignes, même lorsque l'utilisateur est absent lors de la distribution de l'objet ;
- il permet une utilisation souple et partagée des consignes entre les utilisateurs, offrant ainsi un service de mise à disposition de plusieurs consignes. Chaque consigne est réservable et attribuable temporairement à un utilisateur ;
- il permet un fonctionnement « réversible », autrement dit un utilisateur souhaitant renvoyer un objet peut déposer cet objet dans une des consignes 18 et utiliser le dispositif de déverrouillage 22 selon l'invention pour fermer la consigne ; un distributeur peut alors récupérer cet objet, par exemple lors d'une de ses tournées de distribution périodiques.

[0114] L'invention est décrite dans ce qui précède à titre d'exemple. Il est entendu que l'homme du métier est à même de réaliser différentes variantes de réalisation de l'invention sans pour autant sortir du cadre de l'invention définie par les revendications.

Revendications

1. Système (1) de distribution d'objets comprenant :

- au moins un équipement (10) de réception d'objets, le ou chaque équipement (10) comprenant au moins une consigne (18) munie d'un ouvrant (20) formant accès à un espace intérieur de la consigne (18) destiné à recevoir un objet, l'équipement (10) comprenant en outre un dispositif (22) de déverrouillage de l'ouvrant (20), une serrure électronique (24) étant agencée au sein de la consigne (18), le dispositif de déverrouillage (22) comprenant la serrure électronique (24) et un module de commande (26) relié à la serrure électronique (24) via une liaison de données (28), la serrure électronique (24) comprenant des moyens moteurs (30) aptes à verrouiller et déverrouiller l'ouvrant (20) suivant la valeur d'une consigne reçue via la liaison de données (28), le module de commande (26) comprenant un capteur (44) d'un signal (56) comprenant une clef numérique et un composant électronique de reconnaissance (46) permettant d'authentifier la clef numérique, le capteur (44) étant propre à transmettre le signal (56) au composant électronique de reconnaissance

(46), ledit composant électronique de reconnaissance (46) étant relié à la liaison de données (28) et étant alimenté par des moyens d'alimentation électrique (48), l'authentification de la clef numérique par le composant électronique de reconnaissance (46) générant un signal de consigne de désactivation des moyens moteurs (30) pour le déverrouillage de l'ouvrant (20), la serrure électronique (24) comprenant des moyens (32) de détection d'une fermeture de l'ouvrant (20) aptes à émettre un signal de détection de fermeture sur la liaison de données (28), le module de commande (26) comprenant en outre des moyens (50) d'émission d'un signal (62) et des moyens (52) de génération de clefs numériques reliés aux moyens d'alimentation électrique (50), au composant électronique de reconnaissance (46) et aux moyens d'émission (50), les moyens de génération (52) étant propres à générer une clef numérique unique à chaque fermeture de l'ouvrant (20), le signal émis (62) comportant la clef numérique unique générée, le composant électronique de reconnaissance (46) étant propre à authentifier la clef numérique reçue par comparaison avec la clef numérique unique générée ;

- deux dispositifs de communication (12A, 12B) propre à émettre un signal (56) comprenant une clef numérique, le signal (56) étant apte à être capté par le capteur (44) du ou d'un des dispositif(s) de déverrouillage (22) et analysé par le composant électronique de reconnaissance (46) dudit dispositif de déverrouillage (22), chaque dispositif de communication (12A, 12B) comprenant des moyens (66) de réception de données adaptés pour communiquer avec les moyens d'émission (50) du dispositif de déverrouillage (22) de sorte à recevoir la ou les clef(s) numérique(s) générée(s) par le module de commande (26) dudit dispositif (22) ;

- un ensemble (14) de stockage de données, relié à chaque dispositif de communication (12A, 12B) via un réseau de communication (16), l'ensemble (14) de stockage de données étant propre à stocker au moins une clef numérique destinée, après analyse par le composant électronique (46) du module de commande (26), à déverrouiller la ou une des consigne(s) (18) de l'équipement (10) de réception d'objets,

le système (1) de distribution étant **caractérisé en ce que** l'ensemble de stockage (14) est propre à transmettre, à un premier (12A) desdits dispositifs de communication, la ou chaque clef numérique fournie par un deuxième (12B) desdits dispositifs de communication, et, pour la ou chaque clef numérique reçue, à générer un message de

notification indicatif de la présence d'un objet dans la ou une des consigne(s) (18) et à transmettre ce message de notification au premier dispositif de communication (12A), et

en ce que le composant électronique de reconnaissance (46) est propre, pour chaque consigne (18), à remplacer dans l'ensemble (14) de stockage de données une éventuelle clef numérique déjà stockée par la clef numérique unique nouvellement générée lors de la fermeture de l'ouvrant (20) de la consigne (18).

2. Système (1) selon la revendication 1, **caractérisé en ce que** le module de commande (26) comprend en outre un composant (54) de codage de données connecté d'une part entre le capteur (44) et le composant électronique de reconnaissance (46) et d'autre part entre les moyens (52) de génération de clefs numériques et les moyens (50) d'émission d'un signal, le composant de codage (54) étant propre à coder les clefs numériques générées par les moyens de génération (52) et à transmettre les clefs numériques codées aux moyens d'émission (50), le composant de codage (54) étant propre à décoder une clef numérique codée contenue dans un signal (56) reçu par le capteur (44) et à transmettre la clef numérique décodée au composant électronique de reconnaissance (46).
3. Système (1) selon l'une des revendications 1 ou 2, **caractérisé en ce que** le composant électronique de reconnaissance (46) comprend une horloge électronique (60) **en ce qu'**une information d'horodatage est associée à la clef numérique unique générée et **en ce que** le composant électronique de reconnaissance (46) n'est propre à authentifier une clef numérique reçue par comparaison avec la clef numérique unique générée que pendant une durée prédéterminée.
4. Système (1) selon la revendication 1, **caractérisé en ce que** le module de commande (26) est agencé au sein de la consigne (18).
5. Système (1) selon la revendication 1, **caractérisé en ce que** le ou chaque équipement (10) comprend une pluralité de consignes (18), chaque consigne (18) étant munie d'un ouvrant (20), et **en ce que** le dispositif de déverrouillage (22) comprend une pluralité de serrures électroniques (24), chaque serrure électronique (24) étant agencée au sein d'une des consigne(s) (18) et étant apte à verrouiller et déverrouiller l'ouvrant (20) de cette consigne (18), le module de commande (26) étant relié à chaque serrure électronique (24) via une liaison de données (28) et étant propre à générer une clef numérique unique à

chaque fermeture d'un des ouvrants (20).

6. Système (1) selon la revendication 1, **caractérisé en ce que** l'ensemble (14) de stockage de données comprend un module (24) de gestion de la disponibilité des consignes (18), le module (24) comportant une table (96) de stockage d'une pluralité de bulletins de consignation, chaque bulletin de consignation étant associé à l'une des consignes (18) et étant apte à prendre une première valeur correspondant à un état libre de la consigne (18), et une deuxième valeur correspondant à un état occupé de la consigne (18). 5
7. Système (1) de distribution d'objets selon la revendication 1, **caractérisé en ce que** le premier dispositif de communication (12A) est muni de moyens (74) d'acquisition de données comprenant une interface utilisateur (76) et une application (78A) stockée au sein du premier dispositif de communication (12A). 10 20
8. Système (1) de distribution d'objets selon la revendication 7, **caractérisé en ce que** l'ensemble de stockage (14) est propre à être relié, via le réseau de communication (16), à une base de données (17) de destinataires, la base de données (17) de destinataires comprenant des enregistrements préalablement validés comme des valeurs d'authentification de destinataires, et **en ce que** les moyens (74) d'acquisition de données du premier dispositif de communication (12A) sont propres, via l'interface utilisateur (76), à recevoir une entrée d'identification d'un utilisateur, l'ensemble de stockage (14) étant propre à transmettre, au premier dispositif de communication (12A), la ou chaque clef numérique reçue uniquement si l'entrée d'identification correspond à un des enregistrements de la base de données (17) de destinataires. 25 30 35 40
9. Système (1) de distribution d'objets selon la revendication 7 ou 8, dans lequel les moyens (74) d'acquisition de données du premier dispositif de communication (12A) correspondent à des instructions de produit programme d'ordinateur téléchargeable depuis un réseau de communication (16) et/ou enregistré sur un support lisible par ordinateur et/ou exécutable par un processeur (70), lorsque le produit programme est exécuté sur ledit dispositif de communication (12A). 45 50

Patentansprüche

1. System (1) zum Verteilen von Objekten, umfassend: 55
 - mindestens eine Ausrüstung (10) zur Aufnahme von Objekten, wobei die oder jede Ausrüs-

tung (10) mindestens ein Schließfach (18) umfasst, das mit einer Öffnung (20) versehen ist, die einen Zugang zu einem Innenraum des Schließfachs (18) bildet, der zur Aufnahme eines Objekts vorgesehen ist, wobei die Ausrüstung (10) ferner eine Vorrichtung (22) zum Entriegeln der Öffnung (20) umfasst, wobei innerhalb des Schließfachs (18) ein elektronisches Schloss (24) angeordnet ist, wobei die Entriegelungsvorrichtung (22) das elektronische Schloss (24) und ein Steuermodul (26) umfasst, das über eine Datenverbindung (28) mit dem elektronischen Schloss (24) verbunden ist, wobei das elektronische Schloss (24) Antriebsmittel (30) umfasst, die geeignet sind, die Öffnung (20) zu verriegeln und zu entriegeln entsprechend dem Wert eines über die Datenverbindung (28) empfangenen Schließfachs, wobei das Steuermodul (26) einen Sensor (44) eines Signals (56) umfasst, das einen digitalen Schlüssel und eine elektronische Erkennungskomponente (46) umfasst, die die Authentifizierung des digitalen Schlüssels ermöglicht, wobei der Sensor (44) das Signal (56) an die elektronische Erkennungskomponente (46) übertragen kann, wobei die elektronische Erkennungskomponente (46) mit der Datenverbindung (28) verbunden ist und über Mittel zur elektrischen Stromversorgung (48) mit Strom versorgt wird, wobei die Authentifizierung des digitalen Schlüssels durch die elektronische Erkennungskomponente (46) ein Signal des Schließfachs zur Deaktivierung der Antriebsmittel (30) zum Entriegeln der Öffnung (20) erzeugt, wobei das elektronische Schloss (24) Mittel (32) zum Erkennen eines Schließens der Öffnung (20) umfasst, die geeignet sind, ein Schließerkennungssignal auf der Datenverbindung (28) auszugeben, wobei das Steuermodul (26) ferner Mittel (50) zum Übertragen eines Signals (62) und Mittel (52) zum Erzeugen digitaler Schlüssel umfasst, die mit den Mitteln zur elektrischen Stromversorgung (50), der elektronischen Erkennungskomponente (46) und den Übertragungsmitteln (50) verbunden sind, wobei die Erzeugungsmittel (52) in der Lage sind, bei jedem Schließen der Öffnung (20) einen eindeutigen digitalen Schlüssel zu erzeugen, wobei das gesendete Signal (62) den erzeugten eindeutigen digitalen Schlüssel umfasst, wobei die elektronische Erkennungskomponente (46) in der Lage ist, den empfangenen digitalen Schlüssel durch Vergleich mit dem erzeugten eindeutigen digitalen Schlüssel zu authentifizieren;

- zwei Kommunikationsvorrichtungen (12A, 12B), die in der Lage sind, ein Signal (56) zu übertragen, das einen digitalen Schlüssel umfasst, wobei das Signal (56) geeignet ist, vom

- Sensor (44) der einen oder einer der Entriegelungsvorrichtungen (22) erfasst zu werden und durch die elektronische Erkennungskomponente (46) der Entriegelungsvorrichtung (22) analysiert zu werden, wobei jede Kommunikationsvorrichtung (12A, 12B) Mittel (66) zum Empfangen von Daten umfasst, die für die Kommunikation mit den Übertragungsmitteln (50) der Entriegelungsvorrichtung (22) geeignet sind, um den/die vom Steuermodul (26) der Vorrichtung (22) erzeugten digitalen Schlüssel zu empfangen;
- eine Datenspeicherbaugruppe (14), die über ein Kommunikationsnetzwerk (16) mit jeder Kommunikationsvorrichtung (12A, 12B) verbunden ist, wobei die Datenspeicherbaugruppe (14) in der Lage ist, nach der Analyse durch die elektronische Komponente (46) des Steuermoduls (26) mindestens einen vorgesehenen digitalen Schlüssel zu speichern, um das oder eines der Schließfächer (18) der Ausrüstung (10) zur Aufnahme von Objekten zu entriegeln, wobei das Verteilungssystem (1) **dadurch gekennzeichnet ist, dass** die Speicherbaugruppe (14) in der Lage ist, den oder jeden digitalen Schlüssel, der von einer zweiten (12B) der Kommunikationsvorrichtungen bereitgestellt wird, an eine erste (12A) der Kommunikationsvorrichtungen zu übertragen und für den oder jeden empfangenen digitalen Schlüssel eine Benachrichtigungsnachricht zu erzeugen, die auf die Anwesenheit eines Objekts in dem oder einem der Schließfächer (18) hinweist, und diese Benachrichtigungsnachricht an die erste Kommunikationsvorrichtung (12A) zu übermitteln, und **dadurch, dass** die elektronische Erkennungskomponente (46) in der Lage ist, für jedes Schließfach (18), einen möglichen bereits gespeicherten digitalen Schlüssel in der Datenspeicherbaugruppe (14) durch den eindeutigen digitalen Schlüssel zu ersetzen, der beim Schließen der Öffnung (20) des Schließfachs (18) neu erzeugt wird.
2. System (1) nach Anspruch 1, **dadurch gekennzeichnet, dass** das Steuermodul (26) ferner eine Datenkodierungskomponente (54) umfasst, die einerseits zwischen dem Sensor (44) und der elektronischen Erkennungskomponente (46) und andererseits zwischen den Mitteln (52) zum Erzeugen digitaler Schlüssel und den Mitteln (50) zum Übertragen eines Signals geschaltet ist, wobei die Kodierungskomponente (54) in der Lage ist, die von den Erzeugungsmitteln (52) erzeugten digitalen Schlüssel zu kodieren und die kodierten digitalen Schlüssel durch die Übertragungsmittel (50) zu übertragen, wobei die Kodierungskomponente (54) in der Lage ist, einen kodierten digitalen Schlüssel zu dekodieren, der in einem vom Sensor (44) empfangenen Signal (56) enthalten ist, und den dekodierten digitalen Schlüssel an die elektronische Erkennungskomponente (46) zu übertragen.
 3. System (1) nach einem der Ansprüche 1 oder 2, **dadurch gekennzeichnet, dass** die elektronische Erkennungskomponente (46) eine elektronische Uhr (60) umfasst, **dadurch dass** eine Zeitstempelinformation einem erzeugten eindeutigen digitalen Schlüssel zugeordnet ist und **dadurch dass** die elektronische Erkennungskomponente (46) in der Lage ist, einen empfangenen digitalen Schlüssel durch Vergleich mit dem erzeugten eindeutigen digitalen Schlüssel nur für eine vorgegebene Dauer zu authentifizieren.
 4. System (1) nach Anspruch 1, **dadurch gekennzeichnet, dass** das Steuermodul (26) innerhalb des Schließfachs (18) angeordnet ist.
 5. System (1) nach Anspruch 1, **dadurch gekennzeichnet, dass** die oder jede Ausrüstung (10) eine Vielzahl von Schließfächern (18) umfasst, wobei jedes Schließfach (18) mit einer Öffnung (20) versehen ist, und **dadurch dass** die Entriegelungsvorrichtung (22) eine Vielzahl von elektronischen Schlössern (24) umfasst, wobei jedes elektronische Schloss (24) innerhalb eines der Schließfächer (18) angeordnet ist und geeignet ist, die Öffnung (20) dieses Schließfachs (18) zu verriegeln und zu entriegeln, wobei das Steuermodul (26) über eine Datenverbindung (28) mit jedem elektronischen Schloss (24) verbunden ist, und geeignet ist, bei jedem Schließen einer der Öffnungen (20) einen eindeutigen digitalen Schlüssel zu erzeugen.
 6. System (1) nach Anspruch 1, **dadurch gekennzeichnet, dass** die Datenspeicherbaugruppe (14) ein Modul (24) zum Verwalten der Verfügbarkeit der Schließfächer (18) umfasst, wobei das Modul (24) eine Tabelle (96) zum Speichern einer Vielzahl von Einzahlungsscheinen umfasst, wobei jeder Einzahlungsschein einem der Schließfächer (18) zugeordnet ist und einen ersten Wert annehmen kann, der einem freien Schließfach (18) entspricht, und einen zweiten Wert, der einem belegten Schließfach (18) entspricht.
 7. System (1) zum Verteilen von Objekten nach Anspruch 1, **dadurch gekennzeichnet, dass** die erste Kommunikationsvorrichtung (12A) mit Mitteln (74) zur Datenerfassung ausgestattet ist, die eine Benutzerschnittstelle (76) und eine innerhalb der ersten Kommunikationsvorrichtung (12A) gespeicherte Anwendung (78A) umfasst.

8. System (1) zum Verteilen von Objekten nach Anspruch 7, **dadurch gekennzeichnet, dass** die Speicherbaugruppe (14) über das Kommunikationsnetzwerk (16) mit einer Datenbank (17) von Empfängern verbunden werden kann, wobei die Empfängerdatenbank (17) Aufzeichnungen umfasst, die zuvor als Empfängerauthentifizierungswerte validiert wurden, und **dadurch dass** die Datenerfassungsmittel (74) der ersten Kommunikationsvorrichtung (12A) über die Benutzerschnittstelle (76) in der Lage sind, eine Identifikationseingabe von einem Benutzer zu empfangen, wobei die Speicherbaugruppe (14) in der Lage ist, den oder jeden empfangenen digitalen Schlüssel nur dann an die erste Kommunikationsvorrichtung (12A) zu übertragen, wenn die Identifikationseingabe einem der Aufzeichnungen der Empfängerdatenbank (17) entspricht.
9. System (1) zum Verteilen von Objekten nach Anspruch 7 oder 8, wobei die Datenerfassungsmittel (74) der ersten Kommunikationsvorrichtung (12A) Computerprogrammproduktanweisungen entsprechen, die von einem Kommunikationsnetzwerk (16) heruntergeladen und/oder auf einem computerlesbaren Medium aufgezeichnet werden können und/oder durch einen Prozessor (70) ausführbar sind, wenn das Programmprodukt auf der Kommunikationsvorrichtung (12A) ausgeführt wird.

Claims

1. A system (1) for dispensing objects, comprising:
- at least one piece of equipment (10) for receiving objects, the or each piece of equipment (10) comprising at least one locker (18) provided with an opening panel (20) forming access to an interior space of the locker (18) intended to receive an object, the piece of equipment (10) further comprising a device (22) for unlocking the opening panel (20), an electronic lock (24) being arranged within the locker (18), the unlocking device (22) comprising the electronic lock (24) and a control module (26) connected to the electronic lock (24) via a data link (28), the electronic lock (24) comprising motor means (30) able to lock and unlock the opening panel (20) according to the value of an instruction received via the data link (28), the control module (26) comprising a sensor (44) for a signal (56) comprising a digital key and an electronic recognition component (46) that makes it possible to authenticate the digital key, the sensor (44) being capable of transmitting the signal (56) to the electronic recognition component (46), said electronic recognition component (46) being connected to the

data link (28) and being powered by electrical power supply means (48), the authentication of the digital key by the electronic recognition component (46) generating an instruction signal for disabling the motor means (30) in order to unlock the opening panel (20), the electronic lock (24) comprising means (32) for detecting a closure of the opening panel (20), means which are able to emit a closure detection signal over the data link (28), the control module (26) further comprising means (50) for emitting a signal (62) and means (52) for generating digital keys connected to the electrical power supply means (50), to the electronic recognition component (46) and to the emitting means (50), the generating means (52) being capable of generating a unique digital key each time the opening panel (20) is closed, the emitted signal (62) comprising the unique digital key generated, the electronic recognition component (46) being capable of authenticating the digital key received by comparing it with the unique digital key generated;

- two communication devices (12A, 12B) capable of emitting a signal (56) comprising a digital key, the signal (56) being able to be picked up by the sensor (44) of the one or more unlocking device(s) (22) and analyzed by the electronic recognition component (46) of said unlocking device (22), each communication device (12A, 12B) comprising data reception means (66) suitable for communicating with the emitting means (50) of the unlocking device (22) so as to receive the one or more digital key(s) generated by the control module (26) of said device (22);
- a data storage assembly (14), connected to each communication device (12A, 12B) via a communication network (16), the data storage assembly (14) being capable of storing at least one digital key intended, after analysis by the electronic component (46) of the control module (26), to unlock the or one of the locker(s) (18) of the piece of equipment (10) for receiving objects, the dispensing system (1) being **characterized in that** the storage assembly (14) is capable of transmitting, to a first (12A) one of said communication devices, the or each digital key supplied by a second (12B) one of said communication devices, and, for the or each digital key received, of generating a notification message indicative of the presence of an object in the or one of the locker(s) (18) and of transmitting this notification message to the first communication device (12A), and **in that** the electronic recognition component (46) is capable, for each locker (18), of replacing in the data storage unit (14) a possible digital key already stored by the unique digital key newly generated when the opening panel (20) of the locker (18) is closed.

2. The system (1) according to claim 1, **characterized in that** the control module (26) further comprises a data-encoding component (54) connected between the sensor (44) and the electronic recognition component (46) as well as between the means (52) for generating digital keys and the means (50) for emitting a signal, the encoding component (54) being capable of encoding the digital keys generated by the generating means (52) and of transmitting the encoded digital keys to the emitting means (50), the encoding component (54) being capable of decoding an encoded digital key contained in a signal (56) received by the sensor (44) and of transmitting the decoded digital key to the electronic recognition component (46).

5
10
15
3. The system (1) according to one of claims 1 or 2, **characterized in that** the electronic recognition component (46) comprises an electronic clock (60), **in that** timestamping information is associated with the generated unique digital key, and **in that** the electronic recognition component (46) is only capable of authenticating a received digital key by comparison with the generated unique digital key for a predetermined time period.

20
25
4. The system (1) according to claim 1, **characterized in that** the control module (26) is arranged within the locker (18).

30
5. The system (1) according to claim 1, **characterized in that** the or each piece of equipment (10) comprises a plurality of lockers (18), each locker (18) being provided with an opening panel (20), and **in that** the unlocking device (22) comprises a plurality of electronic locks (24), each electronic lock (24) being arranged within one of the locker(s) (18) and being able to lock and unlock the opening panel (20) of this locker (18), the control module (26) being connected to each electronic lock (24) via a data link (28) and being capable of generating a unique digital key each time one of the opening panels (20) is closed.

35
40
6. The system (1) according to claim 1, **characterized in that** the data storage assembly (14) comprises a module (24) for managing the availability of the lockers (18), the module (24) comprising a table (96) for storing a plurality of storage slips, each storage slip being associated with one of the lockers (18) and being able to adopt a first value corresponding to a free state of the locker (18), and a second value corresponding to an occupied state of the locker (18).

45
50
7. The system (1) for dispensing objects according to claim 1, **characterized in that** the first communication device (12A) is provided with data-acquisition means (74) comprising a user interface (76) and an appli-

55
8. The system (1) for dispensing objects according to claim 7, **characterized in that** the storage assembly (14) is capable of being connected, via the communication network (16), to a database (17) of recipients, the database (17) of recipients comprising records previously validated as recipient authentication values, and **in that** the data-acquisition means (74) of the first communication device (12A) are capable, via the user interface (76), of receiving a user identification input, the storage assembly (14) being capable of transmitting, to the first communication device (12A), the or each digital key received only if the identification input matches one of the records of the database (17) of recipients.

5
9. The system (1) for dispensing objects according to claim 7 or 8, wherein the data-acquisition means (74) of the first communication device (12A) match instructions of a computer program product that can be downloaded from a communication network (16) and/or stored on a computer-readable medium and/or executed by a processor (70), when the program product is executed on said communication device (12A).

30

cation (78A) stored within the first communication device (12A).

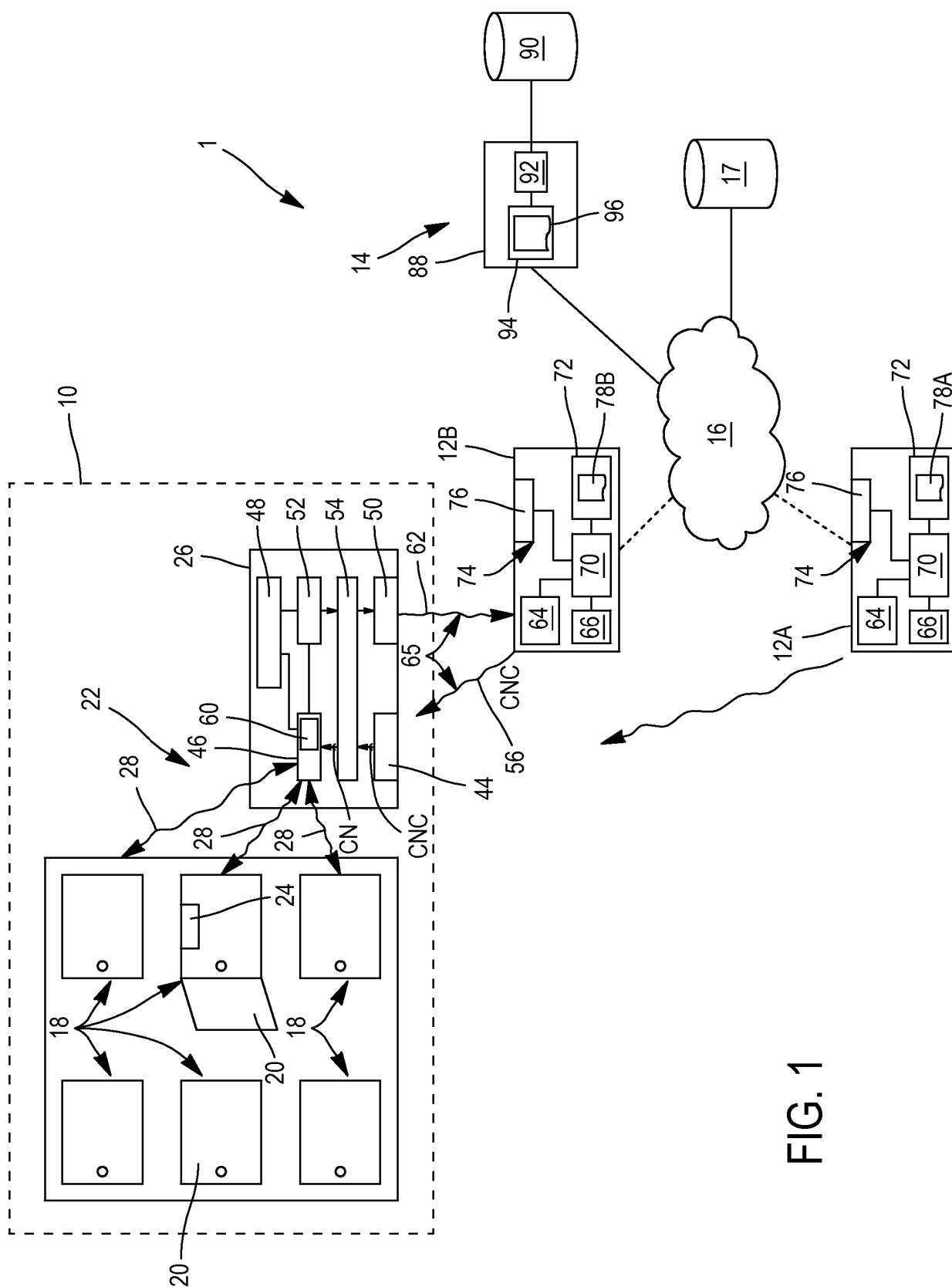


FIG. 1

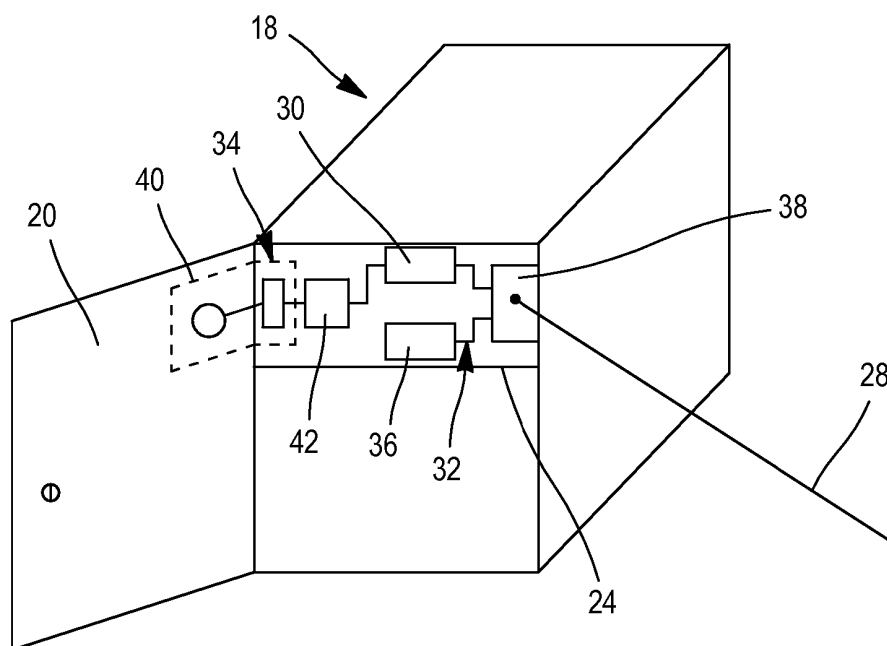


FIG. 2

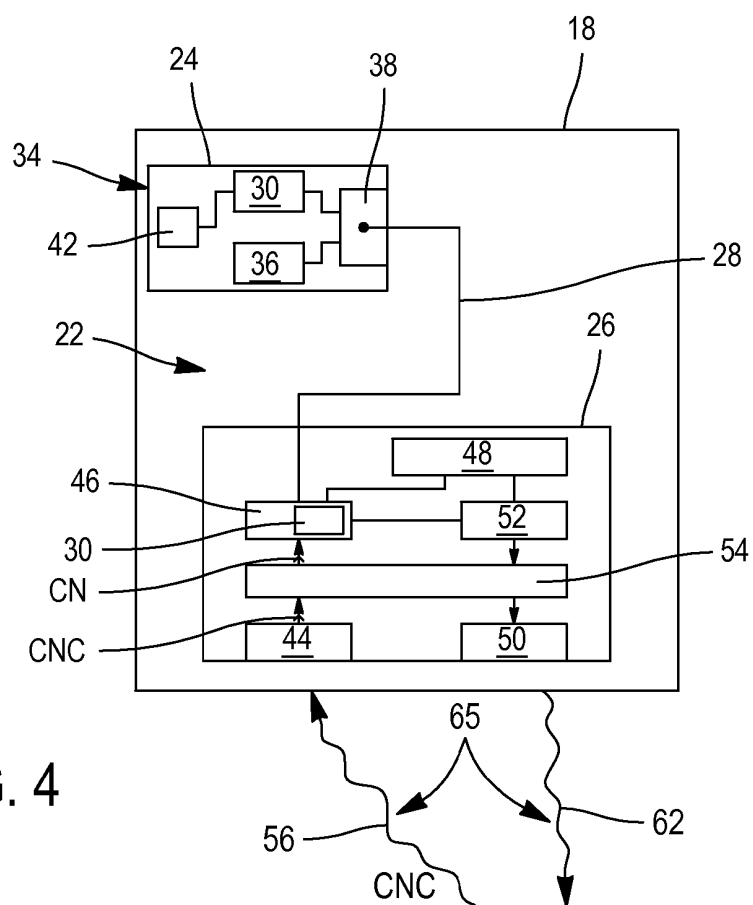


FIG. 4

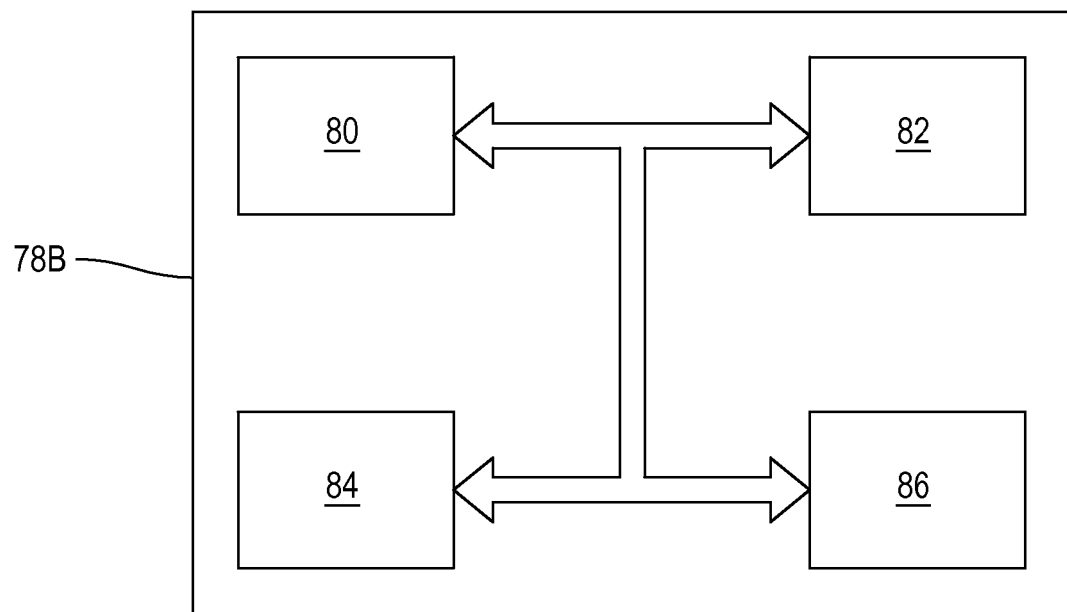


FIG. 3

RÉFÉRENCES CITÉES DANS LA DESCRIPTION

Cette liste de références citées par le demandeur vise uniquement à aider le lecteur et ne fait pas partie du document de brevet européen. Même si le plus grand soin a été accordé à sa conception, des erreurs ou des omissions ne peuvent être exclues et l'OEB décline toute responsabilité à cet égard.

Documents brevets cités dans la description

- EP 2628418 A1 [0003]
- WO 2009018931 A1 [0007]
- WO 2013189721 A1 [0008]
- DE 10164574 [0009]
- WO 2012143634 A1 [0010]