(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 4 075 398 A1**

(12) **DEMANDE DE BREVET EUROPEEN**

(43) Date de publication:
19.10.2022 Bulletin 2022/42

(21) Numéro de dépôt: **22168636.3**

(22) Date de dépôt: **15.04.2022**

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

(52) Classification Coopérative des Brevets (CPC):
G07C 9/00309; G07C 9/00563; G07C 9/00571; G07C 9/00857; G07C 9/26; G07C 2009/0088

(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
Etats d'extension désignés:
BA ME
Etats de validation désignés:
KH MA MD TN

(30) Priorité: **15.04.2021 FR 2103877**

(71) Demandeur: **Vauban Systems SAS**
95000 Cergy (FR)

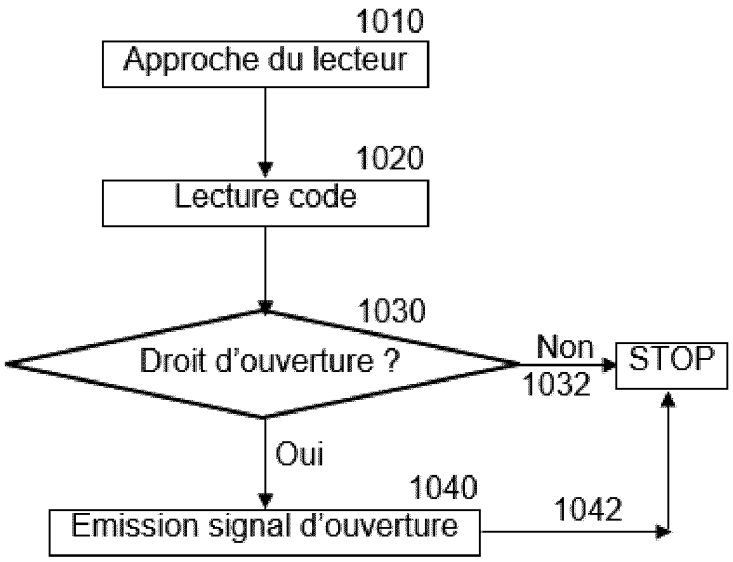
(72) Inventeur: **LIBS, David**
69680 Chassieu (FR)

(74) Mandataire: **Schmidt, Martin Peter**
IXAS Conseil
22 avenue René Cassin
69009 Lyon (FR)

(54) **SYSTEME DE CONTROLE D'ACCES**

(57) Système radioélectrique (1) de contrôle d'accès, comprenant des dispositifs de fermeture (10), des émetteurs-récepteurs (20) portables et un ordinateur central distant (40), caractérisé en ce que :
- chaque dispositif de fermeture (10) comporte un code d'identification visuelle (11) unique et un récepteur Bluetooth (12) configuré pour communiquer avec lesdits émetteur-récepteurs (20) portables,
- chaque émetteur-récepteur (20) portable comporte un microprocesseur (24) configuré pour communiquer avec un lecteur optique (21), un émetteur Bluetooth (22) et une unité de mémoire (23) situés dans ledit émetteur-récepteur (20), ledit émetteur-récepteur (20) portable étant configuré pour communiquer sans fil avec ledit ordinateur central distant (40) et avec le récepteur Bluetooth (12) desdits dispositifs de fermeture (10),
ledit système (1) étant configuré pour exécuter un procédé dans lequel :
- ledit code d'identification visuelle (11) d'un dispositif de fermeture (10) est lu par ledit lecteur optique (21),
- ledit émetteur-récepteur portable vérifie s'il est autorisé à déverrouiller ledit dispositif de fermeture (10),
- si l'émetteur-récepteur portable (20) constate qu'il dispose de cette autorisation, son émetteur Bluetooth (22) émet un signal d'ouverture, qui déclenche le déverrouillage dudit dispositif de fermeture (10).

[Fig. 3]



EP 4 075 398 A1

Description

Domaine technique de l'invention

[0001] L'invention concerne le domaine des dispositifs et systèmes de contrôle d'accès aux bâtiments et aux différentes pièces au sein d'un bâtiment. Plus particulièrement, il concerne les systèmes d'accès comprenant une pluralité de dispositifs de fermeture mécatroniques, qui peuvent être ouverts par les usagers porteurs d'un support d'identification et disposant du droit d'ouvrir un ou plusieurs de ces dispositifs de fermeture. L'invention concerne également un procédé d'utilisation d'un tel système de contrôle d'accès.

Etat de la technique

[0002] On connaît différents dispositifs de fermeture mécatroniques qui sont configurés pour reconnaitre les personnes disposant d'une autorisation d'accès. Pour cela les dispositifs de fermeture coopèrent avec un support d'identification dédié au système, qui est personnel à l'usager et qui reste sous sa garde. Ce support d'identification peut être par exemple un transpondeur ou une carte magnétique ou une carte à puce (« smart card » en anglais) ; ce support d'identification contient les droits d'accès de l'usager ou peut simplement servir à identifier l'usager porteur de ce support. Le support d'identification envoie un signal d'identification au dispositif de fermerture mécatronique pour ouvrir ou fermer la porte. Les autorisations d'accès sont gérées de manière centrale par un ordinateur qui les transmet aux dispositifs de fermeture mécatroniques et / ou aux supports d'identification. Ces dispositifs de fermeture mécatronique existent dans le commerce sous différentes appelations, telle que « fermeture numérique ». Un exemple pour une tel système selon l'état de la technique est connu sous la désignation « Système 3060 ™» de la société SimonsVoss. Des systèmes similaires sont décrits dans US 2014/000 2236 (Viscount Security Systems).

[0003] D'une manière générale, les systèmes de contrôle et d'autorisation d'accès peuvent être conçus avec différents niveaux de sécurité, sachant que tous les sites, et au sein d'un même site toutes les portes, n'ont pas besoin du même niveau de sécurité. Dans une clinique par exemple, on ne protège pas la porte du local à poubelles de la cuisine avec le même degré de sécurité que la porte du local de stockage de produits anésthésiants. En effet, la complexité technique d'un système de contrôle et d'autorisation d'accès, son coût d'investissement, son coût d'installation et son coût d'exploitation dépendent du niveau de sécurité souhaité par l'exploitant du site dans lequel il est installé. D'une manière générale l'état de la technique offre de nombreux systèmes d'un haut degré de complexité, visant à assurer un haut degré de sécurité, alors que la présente invention vise un système aussi simple que possible, facile à installer, qui procure un niveau de sécurité suffisant dans de très nombreux cas, sans viser le plus haut degré de sécurité imaginable.

[0004] L'avantage des dispositifs de fermeture mécatroniques selon l'état de la technique mentionné ci-dessus est qu'ils incorporent une batterie et ne nécessitent pas de cablage ; cela simplifie leur installation. L'inconvénient des systèmes à support d'identification est leur coût d'investissement, et le besoin de programmer le support d'utilisateur pour chaque utilisateur auquel il est confié, qui augmente le coût d'exploitation du système. Par ailleurs, on observe que le support d'identification est assez souvent perdu par le détenteur auquel il a été confié. L'inconvénient de la plupart des systèmes existants est le besoin d'une communication sans fil dédiée entre l'ordinateur central et le dispositif de fermeture mécatronique, qui rend le dispositif de fermeture mécatronique plus complexe, le rend vulnérable contre des cyberattaques, et augmente sa consommation d'energie.

[0005] On connait également de US 2017/0142 581 (Sensormatic Electronics) des systèmes radioélectriques pour le contrôle d'accès dans lesquels l'utilisateur doit scanner avec son téléphone portable un code barre apposé à la porte, et son authentification sera analysée par un ordinateur central ; cette requête (ainsi que la réponse) transite par l'internet et par une centrale de traitement de données au niveau local. Ce système est assez souple pour programmer différents modes d'utilisation, mais il nécessite en plus de l'ordinateur central une centrale de traitement au niveau local, et les données transitent par l'internet, un réseau de télécommunication et/ou un réseau local. Un système similaire est décrit dans US 2015/022 8133 (Illinois Tool Works). Le niveau de sécurité de ce système peut être augmenté encore en modifiant le code affiché à la porte à chaque fermeture, et en envoyant un code confidentiel à usage unique sur le téléphone portable de l'usager habilité ; un tel système est proposé dans EP 3 584 769 A1 (Detec AS).

[0006] Il existe un besoin pour un système de contrôle d'accès plus simple, qui présente, à niveau de sécurité à peu près comparable, les avantages des systèmes existants décrits ci-dessus, sans en présenter les inconvénients. En particulier, on souhaite disposer d'un système qui évite non seulement tout travail de cablage dans les locaux dont l'accès doit être contrôlé, mais encore un système facile à modifier, facile à étendre, et pour lequel la gestion des droits d'accès soit aussi simple que possible.

[0007] En effet, ces droits d'accès se réfèrent souvent non seulement à un seul dispositif de fermeture, mais à plusieurs dispositifs de fermeture au sein d'un système de contrôle d'accès, qui s'étend par exemple à un étage de bureaux, un batiment industriel ou commercial, un site industriel. La gestion de ces droits d'accès pour un grand site avec un grand nombre de portes et d'utilisateurs peut être complexe, et implique la gestion d'un grand nombre de données. De même, l'interrogation envoyée par un dispositif de fermeture à un poste central pour vérifier si l'utilisateur qui se présente devant la porte dispose du

droit d'accès pour l'ouvrir peut impliquer la génération et la gestion d'un grand nombre de signaux ; en tenant compte de la portée différente des différentes voies de transmission sans fil au sein d'un site d'une certaine taille, cela rend le système radioélectrique matériellement et logiciellement complexe, et peut en outre générer un risque d'interférence électromagnétique.

[0008] Comme cela vient d'être évoqué, la présente invention vise à proposer une solution particulièrement simple, qui ne nécessite pas un investissement important, et qui minimise également le nombre de signaux à transmettre au sein du bâtiment ou site concerné.

Objets de l'invention

[0009] Selon l'invention, le problème est résolu par une combinaison de moyens qui sera expliquée ci-dessous, et qui sont réunis dans un système radioélectrique.

[0010] Selon une caractéristique essentielle de l'invention, l'instruction de déverrouillage (déblocage) est transmise d'un émetteur-récepteur portable vers le récepteur d'un dispositif de fermeture par une voie sans fil de type Bluetooth.

[0011] Nous entendons ici par Bluetooth un moyen de transmission de données à courte distance et à faible débit selon un protocole Bluetooth ; cette transmission utilise habituellement des ondes radio d'une bande de fréquence de 2,4 GHz, à faible puissance. Cette voie de transmission inclut notamment une transmission selon la norme BLE (Bluetooth Low Energy), qui est utilisée dans le cadre de la présente invention. La portée de ces signaux BLE ne dépasse typiquement pas 10 mètres ; cela convient pour mettre en œuvre la présente l'invention, sachant que l'invention peut fonctionner avec une portée des signaux Bluetooth plus faible, par exemple de l'ordre d'un mètre. On note que la dénomination Bluetooth est une marque enregistrée.

[0012] Ainsi, chaque dispositif de fermeture faisant partie du système radioélectrique selon l'invention est nécessairement doté d'un récepteur Bluetooth ; il peut s'agir d'un émetteur-récepteur Bluetooth. Par ailleurs, chaque dispositif de fermeture comprend un code d'identification visuelle, unique sur un même réseau. Il est appelé ici « visuel » car l'information qu'il contient peut être lue par des moyens visuels, par opposition aux codes magnétiques ou digitaux. Ce code est attaché au dispositif de fermeture.

[0013] Un premier objet de l'invention est un système radioélectrique de contrôle d'accès, comprenant une pluralité de dispositifs de fermeture, une pluralité d'émetteurs-récepteurs portables et un ordinateur central distant, caractérisé en ce que :

- chaque dispositif de fermeture comporte un code d'identification visuelle unique et un récepteur Bluetooth configuré pour communiquer avec lesdits émetteur-récepteurs portables,
- chaque émetteur-récepteur portable comporte un microprocesseur configuré pour communiquer avec un lecteur optique, un émetteur Bluetooth et une unité dé mémoire situés dans ledit émetteur-récepteur, ledit émetteur-récepteur portable étant configuré pour communiquer sans fil avec ledit ordinateur central distant et avec le récepteur Bluetooth desdits dispositifs de fermeture,

ledit système étant configuré pour exécuter un procédé dans lequel :

- ledit code d'identification visuelle d'un dispositif de fermeture est lu par ledit lecteur optique,
- ledit émetteur-récepteur portable vérifie ensuite s'il dispose de l'autorisation pour déverrouiller ledit dispositif de fermeture,
- si l'émetteur-récepteur portable dispose de cette autorisation, son émetteur Bluetooth émet un signal d'ouverture, qui, après réception par ledit récepteur Bluetooth dudit dispositif de fermeture, déclenche le déverrouillage dudit dispositif de fermeture.

[0014] Selon un mode de réalisation avantageux, la détection dudit code d'identification visuelle déclenche l'exécution d'un logiciel préalablement chargé dans une unité de mémoire dudit microprocesseur de l'émetteur-récepteur portable, ledit logiciel étant configuré pour exécuter ledit procédé.

[0015] Le système radioélectrique comprend un ordinateur central distant. L'adjectif « distant » signifie ici que sa localisation n'a pas d'importance, dans la mesure où l'ordinateur central ne communique qu'avec les émetteurs-récepteurs portables, et par un moyen de communciation sans fil. Le système radioélectrique selon l'invention ne nécessite pas l'intervention de l'ordinateur central distant pour l'autorisation de chaque ouverture d'un moyen de fermeture. Il ne prévoit pas de communication directe entre les dispositifs de fermeture et l'ordinateur central distant.

[0016] Le système radioélectrique selon l'invention est avantageusement configuré pour que l'ordinateur central distant délivre à au moins un émetteur-récepteur portable une autorisation pour émettre, à chaque fois que ledit émetteur-récepteur portable aura lu le code d'identification visuelle d'un moyen de fermeture déterminé, un signal d'ouverture, appelé aussi signal de déverrouillage, pour déverrouiller ledit dispositif de fermeture ; cet envoi peut être limité à certaines plages horaires et/ou certains jours de la semaine et/ou certains dates, ou peut être donné une seule fois.

[0017] Le système radioélectrique selon l'invention est avantageusement configuré pour que ledit ordinateur central distant puisse envoyer un signal à l'émetteur-récepteur portable qui mette fin à l'autorisation délivrée audit émetteur-récepteur portable.

[0018] Selon un mode de réalisation très avantageux de l'invention, ledit dispositif de fermeture comprend une serrure mécatronique. Selon un autre mode de réalisa-

tion très avantageux, ledit dispositif de fermeture ne comporte pas d'autre émetteur et/ou récepteur de signaux radioélectriques que ledit récepteur Bluetooth.

[0019] Un deuxième objet de l'invention est un dispositif de fermeture pour réseau radioélectrique selon l'invention, comprenant un récepteur Bluetooth configuré pour communiquer avec un émetteur-récepteur portable. Selon une variante ledit dispositif de fermeture comporte un émetteur-récepteur Bluetooth.

[0020] Un troisième objet de l'invention est un procédé de déverrouillage d'un dispositif de fermeture selon l'invention, dans lequel : dans une première étape, un utilisateur approche son émetteur-récepteur portable, qui dispose d'un lecteur optique, d'un émetteur Bluetooth et d'un microprocesseur, du code d'identification visuelle attaché à un dispositif de fermeture pourvu d'un récepteur Bluetooth, de manière à ce que ledit lecteur optique puisse lire ledit code d'identification visuelle ; dans une deuxième étape, ledit lecteur optique lit ledit code d'identification visuelle ;

dans une troisième étape ledit microprocesseur vérifie si ledit émetteur-récepteur portable a reçu préalablement à la première étape de l'ordinateur central distant un signal transmis par un moyen sans fil lui conférant le droit de déverrouiller ledit dispositif de fermeture ;
et si ledit émetteur-récepteur portable a reçu ce droit, et seulement dans ce cas, dans une quatrième étape, son émetteur Bluetooth émet un signal qui sera reçu par le récepteur Bluetooth du dispositif de fermeture, et qui ordonne le déverrouillage dudit dispositif de fermeture.

[0021] Dans la troisième étape, « préalablement » signifie « préalablement au déclenchement du procédé de déverrouillage selon l'invention par cet émetteur-récepteur portable » (autrement dit, avant le début de l'exécution du procédé de dévrrouillage), sachant que le déroulement du procédé de déverrouillage selon l'invention en tant que tel n'implique pas d'échange d'informations entre l'émetteur-récepteur portable et l'ordinateur central distant.

[0022] Encore un autre objet de l'invention est un logiciel chargé sur une mémoire d'un émetteur-récepteur portable, spécifiquement configuré pour exécuter le procédé de déverrouillage selon l'invention lorsqu'il est exécuté sur le microprocesseur dudit émetteur-récepteur portable faisant partie du système radioélectrique selon l'invention.

Figures

[0023] L'invention est illustrée à l'aide de plusieurs figures, qui représentent des aspects particuliers de l'invention pour faciliter sa compréhension, mais qui n'ont pas pour vocation à limiter sa portée juridique aux seuls modes de réalisation illustrés.

[Fig. 1] montre de manière schématique un réseau radioélectrique selon l'invention dans une configuration minimale, avec un seul dispositif de fermeture et un seul utilisateur.

[Fig. 2] montre de manière schématique un réseau radioélectrique selon l'invention avec plusieurs dispositfs de fermeture.

[Fig. 3] montre de manière schématique les étapes d'un premier procédé d'utilisation du résau radioélectrique selon l'invention.

[Fig. 4] montre de manière schématique les étapes d'un autre procédé d'utilisation du résau radioélectrique selon l'invention.

[0024] Sur les figures et dans la description qui suit, les repères numériques suivants sont utilisés :

1	Système radioélectrique selon l'invention
10	Dispositif de fermeture
11	Code d'identification visuelle
12	Récepteur Bluetooth
20	Emetteur-récepteur portable
21	Lecteur optique
22	Emetteur Bluetooth
23	Unité de mémoire
24	Microprocesseur
25	Emetteur-récepteur
31	Lecture optique
32	Liaison Bluetooth
35	Communication sans fil bidirectionnelle
40	Ordinateur central distant
45	Emetteur-récepteur de 40

[0025] Les repères numériques à quatre chiffres se rapportent à des étapes de procédé.

Description détaillée

[0026] Le système radioélectrique selon l'invention comprend une pluralité de dipositifs de fermeture dont chacun est associé à un code d'identification visuelle différent qui le distingue des autres. Ce code d'identification visuelle est fixe. De manière préférée ce code est gravé dans une partie visible du dispositif de fermeture, ou imprimé sur une partie visible du dispositif de fermeture. Il peut aussi être gravé ou imprimé sur une plaque ou tout autre support attaché au dispositif de fermeture, par exemple par collage ou encastrement. Dans la mesure où le remplacement du dispositif de fermeture entraîne le remplacement du code d'identification visuelle, on préfère que ledit code soit matériellement intégré dans le dispositif de fermeture, comme cela vient d'être expliqué. Il serait cependant également envisageable de fixer le code à proximité du dispositif de fermeture, par exemple sur la porte, sur l'encadrement de la porte ou sur un mur à côté de la porte.

[0027] Dans le cadre de l'exécution normale du procédé de déverrouillage selon l'invention et de l'utilisation

normale du dispositif et système radioélectrique selon l'invention, il n'est pas prévu de changer ce code. Cela serait théoriquement possible, par exemple en collant une nouvelle étiquette de code sur une ancienne étiquette, mais nécessiterait de reconfigurer l'ordinateur central distant qui devra alors associer ce nouveau code à ce dispositif de ferméture spécifique ; en revanche, aucune intervention ne serait nécessaire sur l'émetteur-récepteur contenu dans le dispositif lui-même. On ne voit cependant pas quel pourrait être l'intérêt de changer ce code, dans la mesure où l'utilisateur ne peut pas utiliser un autre code pour ce dispositif de fermeture, et ne peut pas utiliser ce code avec un autre dispositif de fermeture.

[0028] Avantageusement ledit code d'identification visuelle est un code graphique d'identification selon un format normalisé, par exemple un code de type QR Code. Dans un autre mode de réalisation, qui est moins préféré, il s'agit d'un code alphanumérique.

[0029] Selon une caractéristique essentielle de l'invention, ce code d'identification visuelle est lu par l'émetteur-récepteur portable, qui en déduit le code d'identification alphanumérique associé au moyen de fermeture. Plus précisément, l'émetteur-récepteur comporte un microprocesseur configuré pour déduire du code d'identification visuelle un code d'identification alphanumérique associé au moyen de fermeture, qu'il compare ensuite à une liste de codes d'identification alphanumérique qui lui a été préalablement communiqué ; s'il résulte de cette compraison que l'émetteur-récepteur portable dispose du droit d'ouvrir ce moyen de fermeture au moment où se déroule cette comparaison, il émet un signal codé de déverrouillage qui est transmis au moyen de fermeture par un moyen de transmission sans fil de courte portée.

[0030] Chaque dispositif de fermeture est configuré pour recevoir un signal radioélectrique digital par une voie de transmsission sans fil de courte portée, de préférence selon le protocole Bluetooth, et plus particulièrement selon le protocole Bluetooth Low Energy (en abrégé BLE). Ce protocole utilise une bande passante plus limitée et présente une très faible consommation d'énergie. Il ne nécessite pas d'appairer le récepteur Bluetooth du dispositif de fermeture avec l'émetteur-récepteur Bluetooth du téléphone portable ; cela simplifie considérablement le procédé d'utilisation du système selon l'invention. Le récepteur Bluetooth localisé dans le dispositif de fermeture peut être un émetteur-récepteur Bluetooth ; la fonction émetteur peut être utilisée ou non dans le protocole de communication avec le téléphone portable. Selon un mode de réalisation préféré, le dispositif de fermeture selon l'invention ne comporte pas d'autre émetteur et/ou récepteur de signaux radioélectriques que ledit récepteur (ou émétteur-récepteur) Bluetooth, car cela n'est ni nécessaire ni utile, et augmenterait la consommation énergétique du dispositif de fermeture. Le système radioélectrique selon l'invention ne ne prévoit pas de communication directe entre les dispositifs de fermeture et l'ordinateur central distant.

[0031] Le dispositif de fermeture selon l'invention dispose d'une alimentation électrique autonome. Il est typiquement alimenté par un élément de stockage d'énergie tél qu'une batterie, qui peut être une batterie primaire ou une batterie secondaire ; dans ce dernier cas elle peut être alimentée par une photopile intégrée dans le dispositif. L'utilisation d'un élément de stockage d'énergie permet d'arriver à l'objectif d'avoir un dispositif de fermeture qui ne nécessite pas de cablage lors de son installation.

[0032] Dans un mode de réalisation très préféré de l'invention, le dispositif de fermeture selon l'invention comprend une serrure mécatronique. Les serrures mécatroniques sont connues en tant que telles, et ne seront pas expliquées ici en plus grand détail. Le dispositif de fermeture selon l'invention peut aussi comprendre un dispositif de vérrouillage électromagnétique ; cette solution présente l'inconvénient d'une forte consommation électrique qui ne permet pas de réaliser un dispositif de fermeture autonome en énergie : les dispositifs de vérrouillage électromagnétique nécessitent en règle générale une alimentation électrique externe, et donc un cablage.

[0033] Le signal digital Bluetooth capable de déverouiller le dispositif de fermeture émane d'un dispositif émetteur-récepteur portable mûni d'un microprocesseur associé à une unité de mémoire ; ce dispositif est équipé par ailleurs d'une caméra. Un tel dispositif peut être un dispositif de type téléphone portable et sera ici désigné parfois sous ce terme, sans que cela limite les caracéristiques du dispositif à celles d'un téléphone portable (connu aussi sous le terme « smartphone »). L'émetteur-récepteur portable comporte au moins deux émetteurs-récepteurs radioélectriques de types différents et opérant sur des fréquences et selon des protocoles différents. Il doit être configuré pour communiquer, d'une part, selon le protocole Bluetooth avec les dispositifs de fermeture. D'autre part, il doit être configuré pour communiquer par une liaison sans fil reliée à l'internet et/ou à une liaision de type GSM avec un ordinateur central distant, qui fait églament partie du réseau radioélectrique ; cela sera expliqué ci-dessous en plus grand détail.

[0034] Le système radioélectrique selon l'invention comprend au moins un, et de préférence une pluralité de tels dispositifs émetteurs-récepteurs portables. L'appartenance d'un dispositif émetteur-récepteur portable au système radioélectrique selon l'invention est établie par le chargement et l'activation d'un logiciel spécifique (appelé aussi une « application » spécifique) dans l'unité de mémoire du microprocesseur de l'émetteur-récepteur portable ; ce logiciel contrôle les deux voies de communication sans fil, à savoir vers le dispositif de fermeture et vers l'ordinateur central distant.

[0035] L'appartenance d'un dispositif de fermeture au système radioélectrique est établie par sa configuration logicielle spécifique, qui permet de recevoir et de gérer un signal Bluetooth codé qui provoque le déverrouillage.

[0036] Nous décrivons ici un procédé d'utilisation du système radioélectrique selon l'invention.

[0037] L'utilisateur approche la zone de lecture de la

caméra de son dispositif émetteur-récepteur du code d'identification attaché au dispositif de fermeture qu'il souhaite ouvrir. La caméra prend une prise de vue de ce code d'identification. Ce code est identifié comme un code d'identification appartenant au système radioélectrique. Cette identification active dans le microprocesseur de l'émetteur-récepteur portable un logiciel (application) qui aura été préalablement chargé sur l'unité de mémoire dudit émetteur-récepteur portable, comme cela sera expliqué en plus grand détail ci-dessous. Alternativement, le système est configuré pour que l'utilisateur active d'abord une application spécifique avant de prendre la prise de vue du code d'identification ; il peut être prévu que cette activation nécessite l'entrée d'un identificant, tel qu'un nom d'utilisateur et/ou d'un mot de passe personnels à cet utilisateur.

[0038] Ce logiciel vérifie si l'utilisateur de cet émetteur-récepteur portable dispose du droit d'ouvrir le dispositif de fermeture dont ledit émetteur-récepteur vient de lire le code d'identification. Ce droit d'ouverture pour un dispositif de fermeture spécifique a été préalablement transmis à cet émetteur-récepteur portable de manière codée par l'ordinateur central, et stocké dans l'unité de mémoire dudit émetteur-récepteur portable. Ce stockage peut se faire selon différents protocoles, par exemple sous la forme d'une configuration spécifique du logiciel (application).

[0039] Si le logiciel constate que le propriétaire de l'émetteur-récepteur dispose du droit d'ouvrir le dispositif, ledit émetteur-récepteur envoie un signal codé au dispositif de fermeture dont il vient de lire le code ; ce signal provoque le déblocage (déverrouillage) du moyen de fermeture.

[0040] Si le logiciel constate que le propriétaire de l'émetteur-récepteur portable ne dispose pas du droit d'ouvrir le dispositif, ledit émetteur-récepteur portable n'envoie pas de signal codé au dispositif de fermeture dont il vient de lire le code, et le dispositif de fermeture reste bloqué (fermé).

[0041] L'ordinateur central distant est le gestionnaire des droits d'accès au sein du système radioélectrique. Il est appelé ici « distant » car sa localisation n'a pas d'importance pour le bon fonctionnement du système, dès lors qu'il est configuré pour et capable de communiquer par une liaison sans fil avec les émetteurs-récepteurs portables. Cette communication peut se faire par un moyen et selon un protocole quelconque, par exemple par une liaison internet ou une liaison de téléphonie mobile (par exemple une liaison GSM) ; ces liaisons sans fils entre un téléphone portable et un ordinateur distant sont connues en tant que telles et ne seront pas expliquées ici en plus grand détail.

[0042] Lorsque l'utilisateur reçoit de l'ordinateur central distant l'autorisation d'intégrer son téléphone portable dans le système radioléctrique (cette autorisation peut lui être communiquée par un message SMS ou internet, par exemple), il télécharge ledit logiciel par une liaison internet sans fil avec l'ordinateur central. A titre d'exemple, le message (sms ou courriel) qui lui est envoyé par l'ordinateur central distant peut comporter un lien sur lequel il doit cliquer pour initier le téléchargement et l'installation du logiciel. Par la suite, l'ordinateur central lui délivre les autorisations pour un ou plusieurs dispositifs de fermeture. Pour chaque dispositif de fermeture cette autorisation peut être donnée pour une certaine durée et/ou pour certains jours et/ou pour certaines heures seulement. Cette autorisation peut être annulée ou modifiée par l'ordinateur central à tout moment. La délivrance, la modification ou l'annulation d'une autorisation par l'ordinateur central peut s'accompagner de l'envoi par ledit ordinateur central distant d'un message à l'émetteur-récepteur portable. Cet envoi peut prendre différentes formes ; il peut s'agir notamment d'un courriel, d'un message de type SMS, ou des tout autre type de message.

[0043] La délivrance des autorisations est envoyée à un émetteur-récepteur portable préalablement au déclenchement du procédé de déverrouillage selon l'invention par cet émetteur-récepteur portable : le déroulement du procédé de déverrouillage selon l'invention en tant que tel ne nécessite pas d'échange d'informations entre l'émetteur-récepteur portable et l'ordinateur central distant. Cela est avantageux car ainsi le procédé de déverrouillage peut se dérouler même dans le cas où une liaison sans fil (par exemple par internet) entre l'émetteur-récepteur portable et l'ordinateur central distant ne peut être établie.

[0044] On peut cependant prévoir que le déroulement du procédé de déverrouillage implique un échange d'informations entre l'émetteur-récepteur portable et l'ordinateur central distant : le système peut être configuré de manière à ce que ce mode de réalisation soit sélectionné à chaque fois lorsqu'une liaison sans fil peut être établie entre l'émetteur-récepteur portable et l'ordinateur distant. Dans ce cas, l'émetteur-récepteur portable envoie à l'ordinateur central distant le code d'identification qu'il a déterminé à partir du code d'identification visuelle, et reçoit, s'il est autorisé, en retour un signal codé qu'il transmet, par sa liaison Bluetooth, au dispositif de fermeture. Ce mode de fonctionnement permet de vérifier en temps réel au niveau de l'ordinateur central le droit d'accès du détenteur de l'émetteur-récepteur d'ovurir ce dispositf de fermeture. Cependant, dans la mesure où dans un bâtiment d'une certaine taille la liason sans fil avec un serveur distant ne peut être assurée partout, il est essentiel que le procédé de déverrouillage puisse se dérouler de manière à ne pas nécessiter un échange d'informations entre l'émetteur-récepteur portable et l'ordinateur central distant.

[0045] Ledit signal codé de déverouillage est généré par l'émetteur-récepteur portable si ce dernier n'est pas connecté à l'internet ; dans le cas contraire il peut être généré soit par l'ordinateur central distant (après la transmission à l'ordinateur central du code d'identification alphanumérique que l'émetteur-récepteur portable a extrait du code d'identification visuel) soit par l'émetteur-

récepteur portable (en recherchant ledit code d'identification alphanumérique dans la liste des moyens de fermeture autorisés qui lui a été transmise préalablement par l'ordinateur central). Ce signal codé n'est pas porté à la connaissance de l'utilisateur de l'émetteur-récepteur portable.

[0046] Dans un mode de réalisation avantageux, l'ordinateur central distant donne au téléphone portable l'instruction de requérir, à fréquence régulière ou non, la liste des dispositifs de fermeture autorisés au déverrouillage, assorti d'une date d'expiration de ladite liste. A l'expiration de ladite liste, ou peu avant ce moment, le téléphone portable va requérir une nouvelle liste. Dans le cas où l'ordinateur central distant envoie un ordre d'annulation anticipé d'autorisation, qui peut comporter l'annulation totale de la liste ou la modification de la liste, cet ordre n'a pas d'effet si le téléphone portable n'est pas relié à un réseau sans fil qui supporte cette transmission. Dans ce cas, l'autorisation vaut jusqu'à l'expiration programmée de la liste.

[0047] On peut aussi prévoir que l'envoi d'une nouvelle liste des dispositifs de fermeture autorisés au déverrouillage se fait à l'initiative de l'ordinateur central distant.

[0048] Dans un mode de réalisation particulier de l'invention, le logiciel chargé dans la mémoire du microprocesseur de l'émetteur-récepteur portable procède à une vérification de l'identité du détenteur dudit émetteur-récepteur portable avant de déverrouiller un dispositif de fermeture ; cette procédure peut être appliquée à tous les dispositifs de fermeture de la liste, ou à certains seulement. A cette fin, dans une première variante, le détenteur peut enregistrer une photographie de son visage ou une empreinte digitale, qui est analysée pour en extraire au moins un paramètre biométrique. Ce paramètre biométrique peut être demandé à chaque demande d'ouverture du dispositif de fermeture, et il est ensuite comparé avec une valeur du même paramètre préalablement établie par le même utilisateur. Cette analyse est effectuée par l'émetteur-récepteur, dont le microprocesseur a été convenablement configuré.

[0049] Dans une deuxième variante, qui peut être combinée avec la première, l'émetteur-récepteur portable demande au détenteur d'entrer un code confidentiel qui lui a été communiquée préalablement ; cette entrée se fait sur l'émetteur-récepteur.

[0050] Typiquement, le déverrouillage qui a été déclenché par la réception par le moyen de fermeture du signal codé de déverrouillage est actif uniquement pour un certain laps de temps prédéterminé ; ce dernier, appelé ici « laps de temps court », se situe par exemple entre trois et dix secondes. Cela veut dire que si au cours de ce laps de temps après la réception par le moyen de fermeture du signal codé de déverouillage ledit moyen de fermeture n'est pas ouvert par l'utilisateur, il se verrouille de nouveau. Dans une troisième variante, qui peut être combinée avec chacune des deux autres, le système est configuré de manière à permettre l'envoi d'un signal codé de dévrouillage sélectionné parmi deux signaux de déverouillage différents : l'un qui dévérouille pour un laps de temps court, l'autre qui dévérouille pour un laps de temps plus long, prédéterminé, appelé ici « laps de temps long », qui peut se situer par exemple entre une heure et dix heures, ou qui peut s'étendre jusqu'à une certaine heure, par exemple l'heure de fermeture normale du site ; ainsi, pendant ce laps de temps long, le moyen de fermeture permet le passage libre. Ce passage libre peut s'appliquer par exemple à la porte d'un bureau individuel, d'un bueau à espace ouvert, ou d'un réfectoire.

[0051] Dans cette troisième variante, il est avantageusement prévu que le système puisse être configuré de manière à permettre aux utilisateurs autorisés, ou à certains utilisateurs autorisés, de sélectionner librement s'il souhaitent prévoir à un moment donné le déverrouillage pour un laps de temps court ou long.

[0052] L'invention peut être appliquée notamment au contrôle d'accès par le moyen de portes susceptibles d'être vérrouillées par des dispositifs de fermeture selon l'invention. Le contrôle d'accès peut concerner notamment les différentes portes d'accès à un bâtiment, et à l'intérieur d'un bâtiment, qu'il s'agisse de bureaux, de locaux techniques, ateliers, laboratoires, de couloirs, de garages, de caves, de greniers, de sites de production artisanale ou industrielle, d'entrepôts, de chambres d'hopital, de chambres d'hôtels, d'appartements de vacances ou d'autres établissements de séjour temporaire.

[0053] L'invention présente plusieurs avantages par rapport à l'état de la technique. Elle simplifie considérablement la gestion des droits d'accès. Elle simplifie la construction des dispositifs de fermeture, qui n'ont plus besoin d'être reliés à l'internet ni même à un ordinateur central ou local. Ainsi, le contrôle de l'accès devient indépendant d'une éventuelle perturbation de la liaison radioélectrique entre le dispositif de fermeture et l'ordinateur central. Par ailleurs, dans la mesure où une liaison internet inexistante ne peut faire l'objet d'une cyberattaque, cela améliore le niveau de sécurité global du système radioélectrique.

[0054] L'invention remplace le support d'identification dédié, qui doit être fourni à l'usager du système radioélectrique, et peut être perdu facilement, par un objet propre à son détenteur, qui présente pour lui une utilité fonctionnelle très variée et dont il prendra soin, à savoir son téléphone portable, et dont la perte ou le vol éventuel sera immédiatement détecté.

[0055] L'invention simplifie la gestion des droits d'accès car les supports d'identification de type transpondeur ou carte à puce selon l'état de la technique ne peuvent pas être reprogrammés à distance, contrairement au support d'identification du système radioélectrique selon l'invention. Par ailleurs, contrairement aux systèmes selon l'état de la technique, le système radioélectrique selon l'invention ne nécessite pas l'intervention de l'ordinateur central pour l'autorisation de chaque ouverture d'un moyen de fermeture : l'ordinateur central n'intervient que pour activer et désactiver le logiciel de communication chargé dans la mémoire de l'émetteur-récepteur porta-

ble, et pour établir, modifier ou retirer le droit d'accès pour un moyen de fermeture donné, mais pas pour son ouverture ou déverrouillage.

[0056] A l'instar du support d'identification dédié, n'importe quel détenteur (appelé ici « détenteur accidentel ») du support d'identification pourra l'utiliser pour ovrir un moyen de fermeture donné (à condition d'avoir connaissance de cette possibilité). Mais contrairement aux supports d'identification de l'état de la technique, le système selon l'invention peut être doté d'une fonction supplémentaire d'identification biométrique du détenteur, ce qui transfère la possibilité d'ouvrir ou déverrouiller le moyen de fermeture du détenteur réel (qui peut être un détenteur accidentel) du téléphone portable à son détenteur autorisé.

[0057] Et enfin, le système selon l'invention est très facile à installer, à modifier, et à paramétrer. Cela est en particulier dû à l'absence d'une centrale de traitement au niveau local. Le système selon l'invention est indépendant d'un système de contrôle d'accès déjà existant, tant que le dispositif de fermeture est capable de recevoir des signaux par un réseau de faible portée, tel que Bluetooth. En particulier, il est très facile d'ajouter des dispositifs de fermeture supplémentaires au réseau. Le système selon l'invention peut également s'intégrer à un système de contrôle d'accès déjà existant sur le site, afin de gérer facilement et de la même manière pour l'exploitation, des droits d'accès.

[0058] Nous décrivons ici un mode de réalisation particulier, en nous référant aux figures.

[0059] La figure 1 montre de manière schématique un réseau radioélectrique **1** selon l'invention dans sa forme la plus simple. Il comprend un dispositif de fermeture **10**, sur lequel a été fixé un code d'identification visuelle **11.** Le dispositif de fermeture comprend un récepteur Bluetooth **12.**

[0060] Le réseau radioélectrique **1** selon l'invention comprend par ailleurs un dispositif émetteur-récepteur portable **20**, qui dispose d'une caméra **21**, d'un émetteur Bluetooth **22**, d'un microprocesseur **24** en communication avec une unité de mémoire **23**, et d'un émetteur-récepteur **25** capable de communiquer sans fil avec un ordinateur central distant **40.** Ce dernier possède un émetteur-récepteur **45**, ou est relié à un tel émetteur-récepteur.

[0061] La figure 1 montre également des liaisons de communication, sachant que les flèches pointillées ou interrompues désignent des liaisons sans fil. La liaison **35** entre l'émetteur-récepteur **45** de l'ordinateur distant **40** et l'émetteur-récepteur portable **25** est typiquement une liaison de type internet. Comme indiqué ci-dessus, cette liaison n'est utilisée qu'occasionnellement, lorsque l'ordinateur central distant **40** attribue des droits d'accès à un émetteur-receveur portable **20**, ou lorsqu'il modifie ou annulle les droits d'accès préalablement attribuées à un émetteur-récepteur portable **20.** Cette liaison internet **35** peut être convenablement sécurisée, par exemple par l'utilisation d'un protocole de chiffrement (cryptage).

[0062] Le repère **32** désigne la liaison sans fil entre l'émetteur Bluetooth **22** de l'émetteur-récepteur portable **20** et le récepteur Bluetooth **12** du dispositif de fermeture **10.** Cette liaison envoie des signaux convenablement codés, qui provoquent le déblocage (déverrouillage) du dispositif de fermeture **10.** Ces signaux sont avantageusement cryptés, par exemple par un protocole de cryptage de type AES à 128 bits.

[0063] Le repère **31** désigne la lecture optique du code d'identification visuelle **11** par le lecteur optique **21** de l'émetteur-récepteur portable **20.** On note que dans le mode de réalisation représenté sur cette figure le dispositif de fermeture **20** n'émet aucun signal électronique, il n'a besoin que de recevoir des signaux ; ces signaux sont de faible portée, tel qu'un signal Bluetooth. Son code d'identification visuelle **11** est visible en permanence, mais seul un émetteur-récepteur portable sur lequel a été chargé le logiciel spécifique, et qui a reçu le droit d'ouverture pour ce dispositif de fermeture spécifique, peut émettre le signal d'ouverture **32.**

[0064] La figure 2 montre un système qui comporte les trois mêmes types de dispositifs que ceux représentés sur la figure 1, qui sont représentés de manière simplifiée. La différence est que ce système comporte plusieurs dispositifs de fermeture **10a**,**10b**,**10c**,**10d**, et plusieurs émetteurs-récepteurs portables **20a**,**20b**,**20c**,**20d**,**20e**, **20f** ; l'ordinateur central distant **30** est au nombre d'un, car cela suffit et contribue à la simplicité du système radioélectrique selon l'invention. On note à cet égard que quel que soit le nombre de dispositifs de fermeture **10** et le nombre d'émetteurs-récepteurs portables **20**, et quelle que soit la distance sur laquelle s'étend ledit réseau radioélectrique, on n'a pas besoin d'un deuxième ordinateur central distant, et on n'a pas non plus besoin d'une centrale de traitement des données au niveau local.

[0065] On note que sur la figure 2, plusieurs communications sont en cours entre les trois types de dispositifs qui constituent le réseau radioélectrique.

[0066] L'émetteur-récepteur portable **20c** est en train de lire le code du dispositif de fermeture **10d**; l'émetteur-récepteur portable **20b** est en train d'envoyer le signal d'ouverture au dispositif de fermeture **10c** ; l'ordinateur central distant **30** est en train d'envoyer un signal **35** à l'émetteur-récepteur **20f** pour modifier ses droits d'accès. On note également que certains émetteurs-récepteurs **20a**,**20d**,**20e** font partie du réseau radioélectrique, dans la mesure où le logiciel (application) spécifique, qui est activé par la lecture du code visuel, a été chargé dans l'unité de mémoire de leur microprocesseur, mais en ce moment lesdits émetteurs-récepteurs portables **20a**,**20d**,**20e** ne participent pas activement au réseau radioélectrique en tant qu'émetteurs-récepteurs.

[0067] De même, font partie du réseau radioélectrique certains dispositifs de fermeture **10a**,**10b**, qui sont configurés pour recevoir un signal d'ouverture émanant d'un émetteur-récepteur portable faisant partie du réseau radioélectrique et disposant des droits d'ouverture pour ces dispositfs de fermeture, mais en ce moment, ces dispo-

sitifs ne sont pas sollicités par un signal d'ouverture.

[0068] Nous décrivons ici en relation avec la figure 3 un procédé d'utilisation du réseau radioélectrique selon l'invention, avec plusieurs variantes.

[0069] Nous décrivons d'abord un procédé de déverrouillage d'un dispositif de fermeture selon l'invention. Dans une première étape **1010**, un utilisateur approche son émetteur-récepteur portable **20**, qui dispose d'un lecteur optique **21**, d'un émetteur Bluetooth **2**2 et d'un microprocesseur **24**, du code d'identification visuelle **11** attaché à un dispositif de fermeture **10** pourvu d'un récepteur Bluetooth **12**, de manière à ce que ledit lecteur optique **21** puisse lire ledit code d'identification visuelle **11**.

[0070] Dans une deuxième étape **1020**, ledit lecteur optique **21**, qui est en communication fonctionnelle avec ledit microprocesseur **24**, lit ledit code d'identification visuelle **11**. De manière typique, il détermine à partir de ce code d'identification visuelle un code d'identification alphanumérique de ce moyen de fermeture ; ce code est unique et fixe.

[0071] Dans une troisième étape **1030** ledit microprocesseur **24** vérifie si ledit émetteur-récepteur portable **20c** a reçu préalablement par l'ordinateur central distant **40** un signal transmis par un moyen sans fil lui conférant le droit d'ouvrir ledit dispositif de fermeture **10d.**

[0072] Si ledit émetteur-récepteur portable **20c** a reçu ce droit pour le dispositif de fermeture **10d** dont le code d'identification visuelle vient d'être lu par son lecteur optique, et seulement dans ce cas, dans une quatrième étape **1040**, son émetteur Bluetooth **22** émet un signal **32** qui sera reçu par le récepteur Bluetooth **12d** du dispositif de fermeture **10d**, et qui ordonne le déverrouillage dudit dispositif de fermeture **10d.** Ensuite le procédé s'arrête à l'étape **1042.**

[0073] Si à l'étape **1030** il s'avère que ledit émetteur-récepteur portable **20** n'a pas reçu ce droit, le procédé s'arrête à l'étape **1032.** Alternativement, de manière optionnelle (non montré sur les figures), l'émetteur Bluetooth **22** émet un signal qui sera reçu par le récepteur Bluetooth **12** du dispositif de fermeture **10**, et qui ordonne la génération d'un signal visuel (un voyant rouge par exemple) et/ou acoustique qui avertit l'utilisateur du défaut d'autorisation de déverrouillage du dispositif de fermeture **10.**

[0074] Dans une variante de ce procédé (non montreé sur les figures), ledit émetteur-récepteur portable demande à son utilisateur d'entrer une information de type biométrique préalablement à l'émission du signal qui ordonne le déverrouillage du dispositif de fermeture, telle qu'une photographie de son visage ou une empreinte digitale.

[0075] Dans une autre variante de ce procédé (non montré sur les figures), ledit récepteur **12** Bluetooth du dispositif de fermeture **10** est un émetteur-récepteur Bluetooth, configuré pour émettre au moins un signal en direction de l'émetteur-récepteur Bluetooth **22** du téléphone portable **20.** Ce signal peut confirmer l'ouverture du dispositif de fermeture. Il peut aussi comporter une information sur l'état de charge de l'élément de stockage d'énergie du dispositif de fermeture. Ces signaux peuvent être exploités de différentes manières. Le signal de confirmation d'ouverture peut être transmis par le téléphone portable à l'ordinateur central distant, par exemple à des fins de contrôle. Le signal porteur d'une information sur l'etat de charge peut être transmis par le téléphone portable à l'ordinateur central, en tous les cas ou, de préférence, uniquement lorsque cet état de charge est inférieure ou égale à une valeur prédéterminée ; cela permet à l'ordinateur central distant d'informer un gestionnaire local du besoin de maintenane du dispositif de fermeture.

[0076] Indépendemment de ce procédé de déverouillage d'un dispositif de fermeture **10**, l'ordinateur central distant **30** peut toujours communiquer avec l'un quelconque des émetteurs-récepteurs portables **20** pour lui conférer le droit de déverrouiller un dispositif de fermeture **10** donné, ou pour lui retirer le droit de déverrouiller un dispositif de fermeture **10** donné. L'octroi du droit de déverrouillage peut être lié à certaines plages horaires et/ou à certains jours de la semaine et/ou à certaines dates. Il peut aussi être à usage unique. Le logiciel qui doit être préalablement chargé dans une unité de mémoire dudit microprocesseur de l'émetteur-récepteur portable **20** afin que ledit émetteur-récepteur portable **20** puisse faire partie du système radioélectrique **1** selon l'invention, peut être téléchargé à partir dudit ordinateur central distant **40**, ou à partir d'un autre serveur, par exemple d'une plateforme publique de téléchargement d'applications ; dans ce dernier cas il doit être ensuite être activé par l'ordinateur central distant **40.**

[0077] L'ordinateur central distant **40** remplit donc une multitude de fonctions différentes. Il reçoit et stocke les codes d'identification uniques et déclare les dispositifs de fermeture repérés par leur code d'identification unique (attribué en usine) et leur donne un libellé. Il gère les identifiants des utilisateurs autorisés et de leurs émetteur-récepteurs portables. Il déclare les utilisateurs autorisés à intégrer le système radioélectrique, et leur attribue les dispositifs de fermeture qu'ils ont le droit de déverrouiller (éventuellement assorti de restrictions quant à la plage horaire et/ou au jour de la semaine et/ou à la date). Il enregistre les événements transmis par les émetteurs-récepteurs portables (déverouillage d'un dispositif de fermeture, état de l'élément de stockage d'énergie du dispositif de fermeture).

[0078] De même, l'émetteur-récepteur portable remplit une multitude de fonctions. Il dispose de deux émetteurs-récepteurs différents, l'un par la voie Bluetooth, l'autre pour communiquer avec l'ordinateur central distant. Il télécharge et installe le logiciel (application), ce qui l'intègre dans le réseau radioélectrique selon l'invention ; lors de ce téléchargement il est en liaison fonctionnelle avec l'ordinateur central distant. Il s'authentifie auprès de l'ordinateur central distant. Il envoie aux dispositifs de fermeture les signaux Bluetooth ordonnant le déverrouillage (ces signaux sont typiquement codés

et avantageusement cryptés). Le cas échéant il transmet à l'ordinateur central distant les informations de confirmation de déverouillage et sur l'état de charge de la batterie qu'il a éventuellement reçues par l'émetteur Bluetooth du dispositif de fermeture.

[0079] Le dispositif de fermeture reçoit l'ordre de déverouillage par l'émetteur-récepteur Bluetooth portable. Il émet un signal de confirmation du déverrouillage. Dans une variante il peutêtre configuré pour émettre un signal comportant une information sur l'état de charge de sa batterie primaire ou secondaire.

[0080] Nous décrivons ici en relation avec la figure 4 un autre procédé d'utilisation du réseau radioélectrique selon l'invention, avec plusieurs variantes. Ce procédé suppose une liaison internet entre l'émetteur-récepteur potrable et l'ordinateur central distant.

[0081] Dans une première étape **2010** le gestionnaire du système radioélectrique crée un nouvel utilisateur, en enregistrant le numéro de téléphone portable de ce dernier. Dans une deuxième étape **2020** un message SMS est envoyé à l'utilisateur avec un lien d'installation du logiciel (application). Dans une troisième étape **2030** l'utilisateur reçoit le SMS, clique sur le lien et installe l'application. Dans une quatrième étape **2040** l'utilisateur lance l'application pour la première fois. A l'étape **2050** l'ordinateur central distant vérifie si l'utilisateur est déjà enregistré. Si cela n'est pas le cas, à l'étape **2052** l'application (installée sur le téléphone portable) demande **2054** à l'utilisateur de saisir son identifiant (qui peut être son numéro de téléphone portable) et le renvoie à l'ordinateur central distant.

[0082] Si le numéro de téléphone est bien compris dans la liste des utilisateurs autorisés et qu'il est bien en attente d'authentification, à l'étape **2060** l'ordinateur central distant envoie un SMS avec un code d'authentification au téléphone portable. A l'étape **2070** l'utilisateur saisit ce code dans l'application. Ce code est envoyé à l'ordinateur central distant à l'étape **2080** et vérifié. Si le code n'est pas correct, le procédé s'arrêt à l'étape **2082.** Si le code est correct **2074**, l'ordinateur central renvoie à l'étape **2090** au téléphone portable un identifiant unique qui est stocké de manière cryptée sur le téléphone portable **2100.**

[0083] D'une manière plus générale, dans le cadre de l'invention on peut mettre en œuvre plusieurs modes d'utilisation différents.

[0084] Après le premier lancement de l'application par un nouvel utilisateur le système procède à la création d'un compte utilisateur. L'utilisateur reçoit alors un courriel avec un lien de confirmation d'adresse email. Ainsi il peut se connecter à l'application.

[0085] Le traitement d'une demande d'ouverture dépend du fait que l'émetteur-récepteur est connecté ou non à l'internet. Lorsque le'émetter-réceoteur est connecté à l'internet, l'utilisateur lance l'application, se connecte à l'application (typiquement en entrant son nom d'utilisateur et un mot de passe), puis il reçoit la liste des moyens de fermetures autorisées. Il scanne le code d'identification visuelle d'un moyen de fermeture, le microprocesseur de son émetteur-récepteur détermine le code d'identification alphanumérique du moyen de fermeture et l'envoie à l'ordinateur central. Si l'utilisateur est autorisé à ouvrir en ce moment ce moyen de fermeture, l'ordinateur central lui envoie une commande d'ouverture cryptée.

[0086] Lorsque l'émetteur-récepteur n'est pas connecté à l'internet, l'utilisateur lance l'application, se connecte à l'application (typiquement en entrant son nom d'utilisateur et un mot de passe). Il scanne le code d'identification visuelle d'un moyen de fermeture, le microprocesseur de son émetteur-récepteur détermine le code d'identification alphanumérique du moyen de fermeture et recherche ledit code d'identification dans la liste qui lui a été préalablement fournie par l'ordinateur central. Si l'utilisateur est autorisé à ouvrir en ce moment ce moyen de fermeture, l'émetteur-récepteur lui envoie une commande d'ouverture cryptée.

Revendications

1. Système radioélectrique (1) de contrôle d'accès, comprenant une pluralité de dispositifs de fermeture (10), une pluralité d'émetteurs-récepteurs (20) portables et un ordinateur central distant (40), **caractérisé en ce que** :

- chaque dispositif de fermeture (10) comporte un code d'identification visuelle (11) unique et un récepteur Bluetooth (12) configuré pour communiquer avec lesdits émetteur-récepteurs (20) portables,
- chaque émetteur-récepteur (20) portable comporte un microprocesseur (24) configuré pour communiquer avec un lecteur optique (21), un émetteur Bluetooth (22) et une unité de mémoire (23) situés dans ledit émetteur-récepteur (20), ledit émetteur-récepteur (20) portable étant configuré pour communiquer sans fil avec ledit ordinateur central distant (40) et avec le récepteur Bluetooth (12) desdits dispositifs de fermeture (10),

ledit système (1) étant configuré pour exécuter un procédé dans lequel :

- ledit code d'identification visuelle (11) d'un dispositif de fermeture (10) est lu par ledit lecteur optique (21),
- ledit émetteur-récepteur portable vérifie ensuite s'il dispose de l'autorisation pour déverrouiller ledit dispositif de fermeture (10),
- si l'émetteur-récepteur portable (20) constate qu'il dispose de cette autorisation, son émetteur Bluetooth (22) émet un signal d'ouverture, qui, après réception par ledit récepteur Bluetooth

(12) dudit dispositif de fermeture (10), déclenche le déverrouillage dudit dispositif de fermeture (10),
- le système radioélectrique ne nécessite pas l'intervention de l'ordinateur central distant pour l'autorisation de chaque ouverture d'un moyen de fermeture.

2. Système radioélectrique (1) selon la revendication 1, **caractérisé en ce que** la détection dudit code d'identification visuelle déclenche l'execution d'un logiciel préalablement chargé dans une unité de mémoire dudit microprocesseur de l'émetteur-récepteur portable, ledit logiciel étant configuré pour exécuter ledit procédé.

3. Système radioélectrique (1) selon la revendication 1 ou 2, **caractérisé en ce qu'**il est configuré pour que l'ordinateur central distant (40) délivre à au moins un émetteur-récepteur portable une autorisation pour émettre, à chaque foi que ledit émetteur-récepteur portable aura lu le code d'identification visuelle d'un moyen de fermeture déterminé, un signal d'ouverture pour déverrouiller ledit dispositif de fermeture.

4. Système radioélectrique (1) selon l'une quelconque des revendications 1 à 3, **caractérisé en ce qu'**il est configuré pour que ledit ordinateur central distant (40) envoie un signal à l'émetteur-récepteur portable (20) qui met fin à l'autorisation délivrée audit émetteur-récepteur portable.

5. Système radioélectrique (1) selon l'une quelconque des revendications 1 à 4, **caractérisé en ce que** ledit dispositif de fermeture (10) comprend une serrure mécatronique.

6. Système radioélectrique (1) selon l'une quelconque des revendications 1 à 5, **caractérisé en ce que** ledit dispositif de fermeture ne comporte pas d'autre émetteur et/ou récepteur de signaux radioélectriques que ledit récepteur Bluetooth (12).

7. Système radioélectrique selon l'une quelconque des revendications 1 à 6, caractérisé ce qu'il ne prévoit pas de communication directe entre les dispositifs de fermeture et l'ordinateur central distant.

8. Système radioélectrique selon l'une quelconque des revendications 1 à 7, **caractérisé en ce que** lesdits dispositifs de fermeture (10) sont alimentés par un élément de stockage d'énergie tel qu'une batterie et ne nécessitent pas de cablage lors de leur installation.

9. Système radioélectrique selon l'une quelconque des revendications 1 à 8, **caractérisé en ce qu'**il est configuré pour que l'ordinateur central distant envoie, à fréquence régulière ou non, à un émetteur-récepteur donné la liste des dispositifs de fermeture que ledit émetteur-récepteur est autorisé à déverrouiller.

10. Système radioélectrique selon l'uen quelconque des revendications 1 à 9, **caractérisé en ce qu'**il est configuré pour que ledit ordinateur central distant puisse envoyer un signal un émetteur-récepteur portable qui met fin à l'autorisation délivrée audit émetteur-récepteur portable.

11. Dispositif de fermeture (10) pour système radioélectrique selon l'une quelconque des revendications 1 à 10, comprenant un récepteur Bluetooth (12) configuré pour communiquer avec un émetteur-récepteur portable, et comprenant un élément de stockage d'énergie, de manière à ne pas nécessiter un câblage lors de son installation.

12. Dispositif de fermeture selon la revedication 11, **caractérisé en ce qu'**il comprend une serrure mécatronique.

13. Dispositif de fermeture (10) selon la revendication 11 ou 12, **caractérisé en ce qu'**il ne comporte pas d'autre émetteur et/ou récepteur de signaux radioélectriques que ledit récepteur Bluetooth (12).

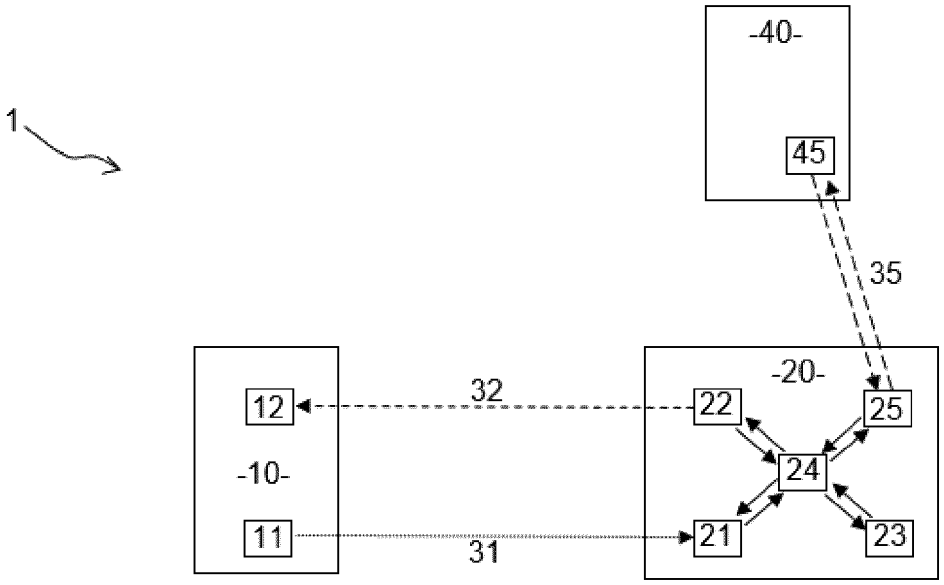
14. Procédé de déverrouillage d'un dispositif de fermeture (10) selon l'une quelconque des revendications 11 à 13 faisant partie d'un système radioélectrique (1) selon l'une quelconque des revendications 1 à 10, dans lequel : dans une première étape (1010), un utilisateur approche son émetteur-récepteur portable (20), qui dispose d'un lecteur optique (21), d'un émetteur Bluetooth (22) et d'un microprocesseur (24), du code d'identification visuelle (11) attaché à un dispositif de fermeture (10) pourvu d'un récepteur Bluetooth (12), de manière à ce que ledit lecteur optique (21) puisse lire ledit code d'identification visuelle (11); dans une deuxième étape (1020), ledit lecteur optique (21) lit ledit code d'identification visuelle (11) ;

dans une troisième étape (1030) ledit microprocesseur (24) vérifie si ledit émetteur-récepteur portable (20) a reçu préalablement à la première étape de l'ordinateur central distant (40) un signal transmis par un moyen sans fil lui conférant le droit de déverrouiller ledit dispositif de fermeture (10) ;
et si ledit émetteur-récepteur portable (20) a reçu ce droit, et seulement dans ce cas, dans une quatrième étape (1040), son émetteur Bluetooth (22) émet un signal qui sera reçu par le récepteur Bluetooth (12) du dispositif de fermeture (10),

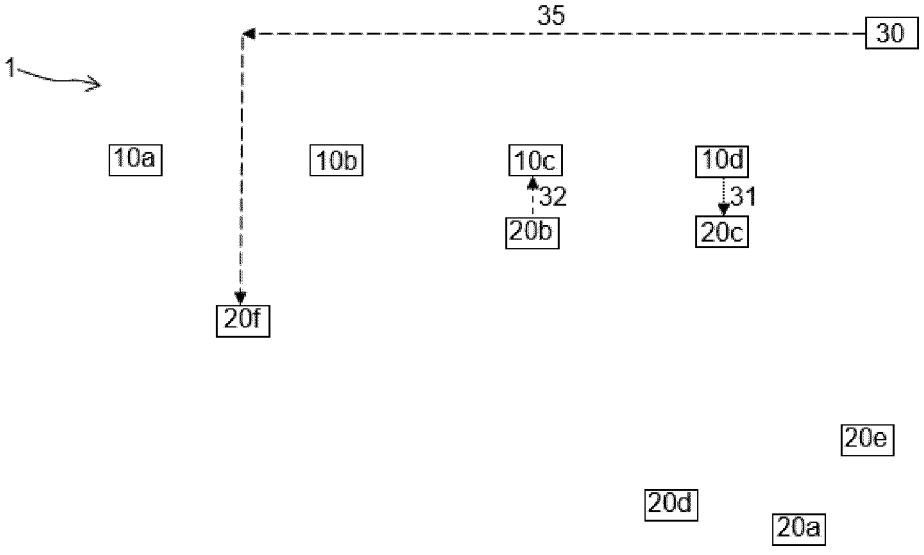
et qui ordonne le déverrouillage dudit dispositif de fermeture (10).

15. Procédé selon la revendication 14, dans lequel ledit émetteur-récepteur portable est configuré pour demander à son utilisateur d'entrer une information de type biométrique préalablement à l'émission du signal qui ordonne le déverrouillage du dispositif de fermeture, telle qu'une photographie de son visage ou une empreinte digitale.

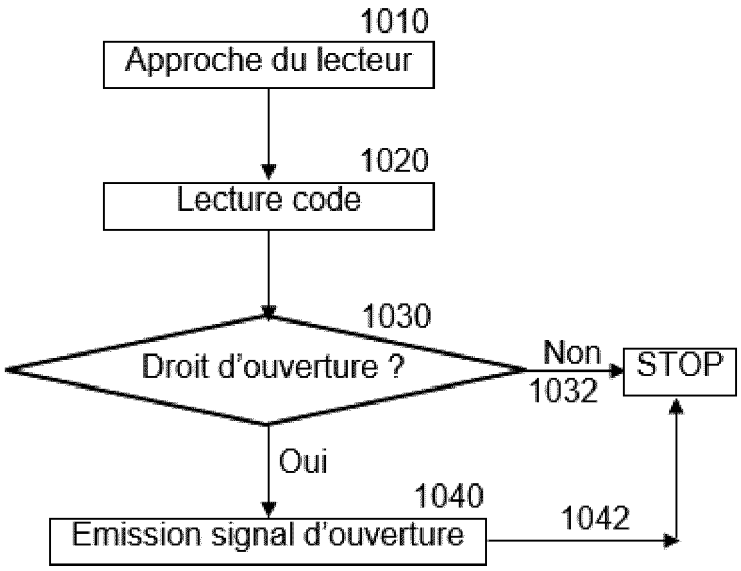
[Fig. 1]


1
-40-
45
35
-20-
12
32
22
25
24
-10-
11
31
21
23

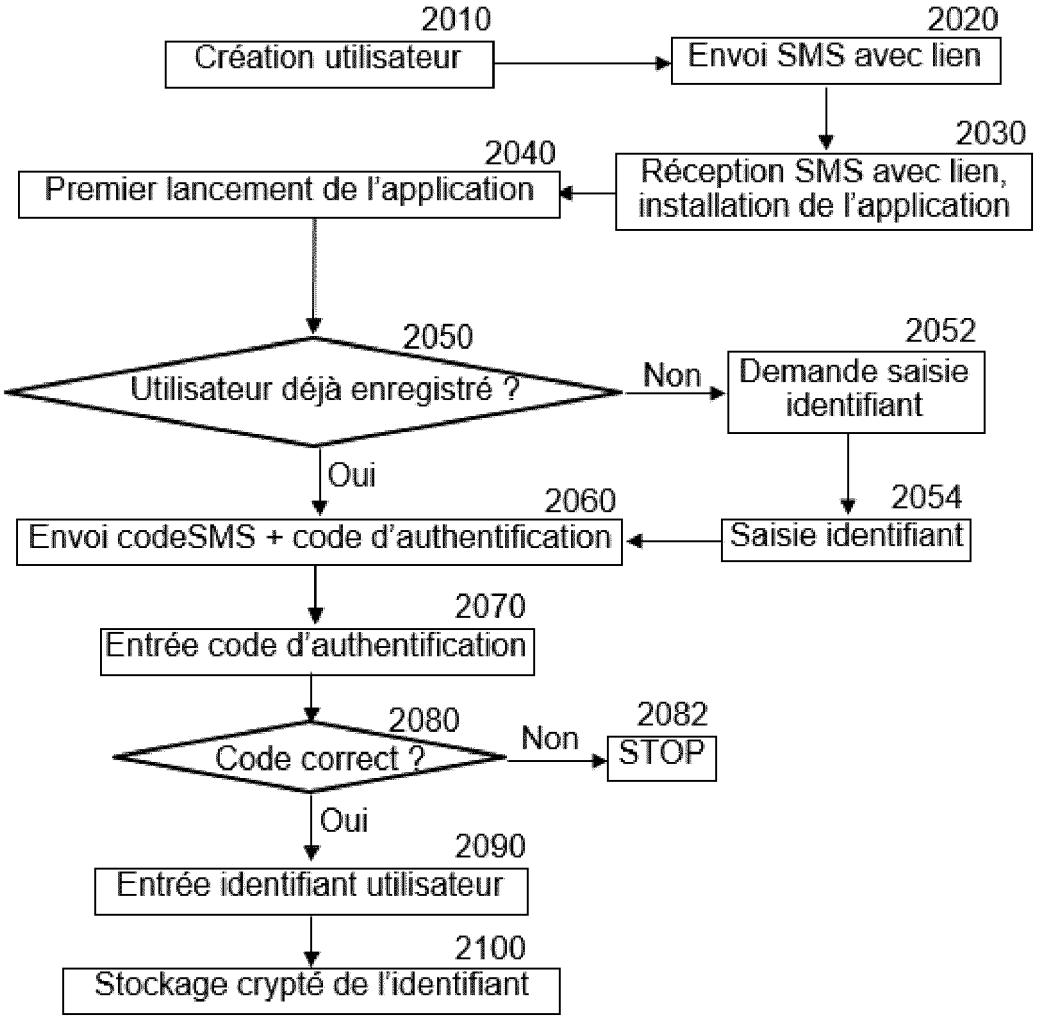
[Fig. 2]


35
30
1
10a
10b
10c
10d
32
31
20b
20c
20f
20e
20d
20a

[Fig. 3]


1010
Approche du lecteur
1020
Lecture code
1030
Droit d'ouverture ?
Non
1032
STOP
Oui
1040
Emission signal d'ouverture
1042

[Fig. 4]


2010
Création utilisateur
2020
Envoi SMS avec lien
2030
Réception SMS avec lien, installation de l'application
2040
Premier lancement de l'application
2050
Utilisateur déjà enregistré ?
Non
2052
Demande saisie identifiant
Oui
2054
Saisie identifiant
2060
Envoi codeSMS + code d'authentification
2070
Entrée code d'authentification
2080
Code correct ?
Non
2082
STOP
Oui
2090
Entrée identifiant utilisateur
2100
Stockage crypté de l'identifiant

Europäisches Patentamt
European Patent Office
Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 22 16 8636

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (IPC)
X	EP 3 528 523 A1 (CARRIER CORP [US]) 21 août 2019 (2019-08-21) * revendications 1-14 * * figures 1-4 * * alinéa [0029] - alinéa [0046] *	1-15	INV. G07C9/00
X	US 2009/324025 A1 (CAMP JR WILLIAM O [US] ET AL) 31 décembre 2009 (2009-12-31) * revendication 16 * * figure 6 * * alinéa [0024] - alinéa [0048] *	1-15	
X	CN 111 932 743 A (SICHUAN SMART BOX IOT TECH CO LTD) 13 novembre 2020 (2020-11-13) * revendications 1-4 * * exemples 1, 2 *	1-15	
X	EP 3 584 769 A1 (DETEC AS [NO]) 25 décembre 2019 (2019-12-25) * revendications 1-9 * * figures 1, 4 * * alinéa [0030] - alinéa [0034] *	1-15	DOMAINES TECHNIQUES RECHERCHES (IPC) G07C
X	US 2016/232729 A1 (ENGEL-DAHAN MANUELA [DE]) 11 août 2016 (2016-08-11) * figures 8-9 * * alinéa [0215] - alinéa [0226] *	1-15	
A	US 2020/329136 A1 (GERHARDT PAUL MICHAEL [US] ET AL) 15 octobre 2020 (2020-10-15) * alinéa [0035] - alinéa [0036] *	1-10	

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
La Haye	2 septembre 2022	Hniene, Badr

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons
.....
& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C02)

ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE RELATIF A LA DEMANDE DE BREVET EUROPEEN NO. EP 22 16 8636

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche européenne visé ci-dessus.
Lesdits members sont contenus au fichier informatique de l'Office européen des brevets à la date du
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets.

02-09-2022

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 3528523 A1	21-08-2019	EP 3528523 A1	21-08-2019
		ES 2867950 T3	21-10-2021
		US 2019260590 A1	22-08-2019
US 2009324025 A1	31-12-2009	CN 102027511 A	20-04-2011
		EP 2283470 A1	16-02-2011
		US 2009324025 A1	31-12-2009
		WO 2009128854 A1	22-10-2009
CN 111932743 A	13-11-2020	AUCUN	
EP 3584769 A1	25-12-2019	EP 3584769 A1	25-12-2019
		EP 3811339 A1	28-04-2021
		WO 2019245383 A1	26-12-2019
US 2016232729 A1	11-08-2016	BR 112016008212 A2	01-08-2017
		CN 105684049 A	15-06-2016
		DE 102013111429 A1	16-04-2015
		DK 3058553 T3	02-09-2019
		EP 3058553 A1	24-08-2016
		EP 3584770 A1	25-12-2019
		ES 2743123 T3	18-02-2020
		HK 1219797 A1	13-04-2017
		JP 6806564 B2	06-01-2021
		JP 2016536498 A	24-11-2016
		JP 2021042669 A	18-03-2021
		KR 20160071403 A	21-06-2016
		PL 3058553 T3	31-01-2020
		RU 2016118668 A	21-11-2017
		US 2016232729 A1	11-08-2016
		WO 2015055344 A1	23-04-2015
US 2020329136 A1	15-10-2020	CA 2834964 A1	08-11-2012
		CN 103635940 A	12-03-2014
		EP 2710562 A1	26-03-2014
		US 2012280783 A1	08-11-2012
		US 2012280789 A1	08-11-2012
		US 2012280790 A1	08-11-2012
		US 2014365773 A1	11-12-2014
		US 2015102906 A1	16-04-2015
		US 2015181014 A1	25-06-2015
		US 2018191889 A1	05-07-2018
		US 2019342443 A1	07-11-2019
		US 2020329136 A1	15-10-2020
		WO 2012151290 A1	08-11-2012

EPO FORM P0460

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82

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

- US 20140002236 A **[0002]**
- US 20170142581 A **[0005]**
- US 20150228133 A **[0005]**
- EP 3584769 A1 **[0005]**