

①9 RÉPUBLIQUE FRANÇAISE  
INSTITUT NATIONAL  
DE LA PROPRIÉTÉ INDUSTRIELLE  
COURBEVOIE

①1 N° de publication : **3 022 092**  
(à n'utiliser que pour les  
commandes de reproduction)

②1 N° d'enregistrement national : **14 01315**

⑤1 Int Cl<sup>8</sup> : **H 04 L 9/32 (2013.01), H 04 W 12/08**

①2 **DEMANDE DE BREVET D'INVENTION**

**A1**

②2 **Date de dépôt** : 10.06.14.

③0 **Priorité** :

④3 **Date de mise à la disposition du public de la demande** : 11.12.15 Bulletin 15/50.

⑤6 **Liste des documents cités dans le rapport de recherche préliminaire** : *Se reporter à la fin du présent fascicule*

⑥0 **Références à d'autres documents nationaux apparentés** :

**Demande(s) d'extension** :

⑦1 **Demandeur(s)** : SADAGOBANE RAMESH — FR.

⑦2 **Inventeur(s)** : SADAGOBANE RAMESH.

⑦3 **Titulaire(s)** : SADAGOBANE RAMESH.

⑦4 **Mandataire(s)** : SADAGOBANE RAMESH.

⑤4 **SYSTEME ET PROCEDE D'IDENTIFICATION AUTOMATIQUE PAR LE TOUCHER ET D'ACCES SANS CLE.**

⑤7 L'invention concerne un dispositif fixe de type lecteur de badge et un dispositif portatif de type badge intégré à une télécommande, dotée de moyens mettant en oeuvre un canal de communication en champ proche exploitant aussi bien un champ magnétique qu'un champ électrique et un canal de communication radiofréquence, pour établir des communications bidirectionnelles entre le dispositif fixe et le dispositif portatif.

Le dispositif fixe comprend une unité de couplage capacitif, à la fois pour détecter l'approche de l'utilisateur et pour transmettre par l'intermédiaire de son corps le signal de réveil et d'interrogation vers le dispositif portatif. Le dispositif portatif qui comporte aussi des moyens de communication radiofréquence RF pour des fonctions de commande à distance, utilise ce canal de transmission existant pour répondre.

Ainsi, l'utilisateur n'a plus besoin d'approcher son badge du lecteur, il suffit qu'il le porte dans une poche de son vêtement et qu'il effleure le lecteur pour que le procédé d'accès se réalise.

Le système selon l'invention est particulièrement destiné au contrôle d'accès dans les bâtiments mais peut aussi s'appliquer à d'autres procédés comme la mise en service et la mise hors service d'équipements qui nécessitent une

sécurisation par l'identification des personnes autorisées.

FR 3 022 092 - A1



- 1 -

La présente invention concerne, de façon générale, un système d'identification automatique par le toucher permettant de donner un accès sans clé « Keyless Entry » et sécurisé à un espace ou à un objet sans l'utilisation d'une clé physique et son procédé.

Plus précisément, l'invention concerne un dispositif portatif de type badge intégré à une 5 télécommande comme il en existe déjà pour la commande à distance des ouvrants, dotée ici, de moyens supplémentaires pour la réception d'un signal de réveil et de demande d'authentification transmis à travers le corps de l'utilisateur par un second dispositif fixe de type lecteur de badge. Le dispositif fixe comprend une unité de couplage capacitif, à la fois pour détecter l'approche de l'utilisateur et pour transmettre par l'intermédiaire de son corps un signal de réveil et d'interrogation 10 vers le dispositif portatif. Le dispositif portatif qui comporte aussi des moyens de communication radiofréquence RF pour sa fonction première de commande à distance, utilise ce canal de transmission existant pour répondre au lecteur.

Dans l'état de la technique, il existe, pour le contrôle d'accès des bâtiments, une solution qui consiste à intégrer un dispositif d'identification (badge) dans un dispositif de commande à 15 distance (télécommande). Ce procédé, connu de l'homme du métier et exploité commercialement, est une simple combinaison de deux technologies dans le but d'obtenir un produit dit « deux en un » (télécommande + badge d'identification). Cette solution n'apporte aucune amélioration pour sécuriser la transmission du code d'identification car bien souvent il s'agit d'un code unique préprogrammé dans la puce du badge qui est transmis automatiquement dès qu'il détecte le champ 20 magnétique émis par le lecteur sous la forme d'un signal modulé appelé « porteuse ». Ce procédé présente l'inconvénient d'être vulnérable aux attaques les plus simples.

Dans un autre état de la technique, les constructeurs automobiles proposent un système d'identification pour le verrouillage et le déverrouillage des portières. Les techniques employées exploitent, pour la transmission du système embarqué dans le véhicule (lecteur) vers la 25 télécommande (dispositif portatif), un champ magnétique avec un signal de réveil modulé en basse fréquence (LF – 100 KHZ à 150KHZ). La télécommande répond en utilisant son émetteur radiofréquence RF en ultra haute fréquence (UHF – 315/434MHZ) avec son identifiant. Ainsi, l'utilisateur peut accéder à son véhicule sans manipuler une clé physique ni actionner sa télécommande. La télécommande doit simplement se trouver dans la zone d'influence du lecteur 30 embarqué dans le véhicule, par exemple dans la poche ou le sac à main de l'utilisateur. La demande de brevet publiée sous le numéro WO 2005104006 décrit un système d'authentification qui s'appuie sur cette technologie.

Cependant, l'état de la technique rencontre trois problèmes qui peuvent être pénalisants pour d'autres applications comme le contrôle d'accès des bâtiments ou d'équipements alimentés par 35 des piles de petites tailles.

Selon un premier problème, l'antenne inductive, qui génère le champ magnétique nécessite une grande quantité d'énergie électrique pour que sa zone d'influence couvre convenablement

- 2 -

l'utilisateur même s'il se tient à plusieurs dizaines de centimètres du véhicule. Les véhicules automobiles sont équipés de batteries capables de fournir une telle énergie mais ce n'est pas le cas des systèmes devant présenter une consommation réduite.

Selon un second problème, il n'existe pas de solution simple pour orienter ou limiter la zone d'influence du champ émis par le lecteur pour garantir que le badge lu est bien celui porté par la  
5 personne qui a initié la lecture. Les constructeurs automobiles, maîtrisant la conception du véhicule dans sa globalité et donc l'environnement dans lequel le système d'identification opère, peuvent positionner les antennes aux endroits stratégiques en utilisant la structure métallique du véhicule de sorte que l'antenne rayonne de manière directionnelle. De cette façon, le système peut déterminer si  
10 la télécommande est à l'intérieur ou à l'extérieur du véhicule. Dans le cas du contrôle d'accès des bâtiments, si l'antenne du lecteur rayonne de manière omnidirectionnelle, son champ risque de réveiller tous les badges situés à proximité et dans toutes les directions. Prenons l'exemple d'un utilisateur qui, en entrant dans son bureau, accroche son manteau avec sa télécommande dans l'une des poches, sur un porte manteau. Supposons que ce porte manteau se trouve juste derrière  
15 le mur sur lequel est installé le lecteur de contrôle d'accès du bureau. Dans une telle situation, où la télécommande se trouve en permanence dans la zone d'influence du lecteur, la protection devient alors totalement inefficace puisque tout le monde peut accéder à cette zone sans y être autorisé.

Selon un troisième problème, le nombre de télécommande/badge pour accéder à un véhicule est en générale limité à deux ou trois unités et ils ne sont associés qu'à un seul véhicule  
20 (récepteur). Pour éviter la copie et la reproduction du code transmis en UHF par la télécommande, on utilise des techniques de « code tournant » ou de « saut de code » (en anglais « Rolling code », « hopping code »). A chaque transmission, un compteur est incrémenté au niveau de la télécommande puis inséré dans la trame de données contenant l'identifiant avant d'être encryptées. Le compteur du récepteur est synchronisé avec celui de la télécommande lors de l'appairage. Le  
25 récepteur n'accepte que les trames qui contiennent une valeur du compteur se trouvant dans une plage limitée par rapport à son propre compteur. Il doit aussi en permanence conserver en mémoire pour chaque télécommande le code d'identification, la clé de cryptage et le compteur. Cette méthode ne convient que si le nombre de télécommandes est limité car elle nécessite beaucoup de ressources aussi bien en mémoire (au moins 16 octets par télécommande) qu'en puissance de  
30 calcul du microprocesseur. De plus il ne peut pas y avoir plusieurs récepteurs pour une même télécommande au risque d'être souvent désynchronisée.

Dans les systèmes de contrôle d'accès des bâtiments, le nombre de télécommande/badge peut atteindre plusieurs dizaines d'unités, voire dans certains cas, des centaines. De plus chaque télécommande/badge doit pouvoir être associé à plusieurs récepteurs et/ou lecteurs de badge. Par  
35 exemple, une entreprise qui équipe ses locaux d'un système de contrôle d'accès doit fournir à tous ses salariés un badge permettant au moins d'entrer dans le bâtiment. Puis le système permet de gérer les niveaux d'accès en restreignant l'accès de certains locaux à un nombre limité de personnes.

- 3 -

Dans un autre état de la technique, il a déjà été décrit des dispositifs utilisant le corps de l'utilisateur à la fois pour l'émission du signal de demande d'authentification par le lecteur vers le dispositif portatif (badge) et pour la réception du signal de réponse émis par le badge. Cette méthode de communication à travers le corps de l'utilisateur exploite exclusivement la conductivité du corps humain pour échanger les données de manière bidirectionnelle. La société « Microchip® Technology Inc. » propose une telle solution dénommée « BodyCom® ».

Nous distinguerons la communication en champ proche basée sur un champ magnétique de la communication à travers le corps humain, qui est aussi une communication en champ proche mais basée sur un signal électrique.

10 L'avantage de la communication par le corps humain par rapport à cette communication de courte distance est que l'utilisateur n'a pas à approcher son badge du lecteur, il suffit qu'il le porte dans une poche de son vêtement et qu'il effleure le lecteur pour que le procédé d'accès se réalise.

Cependant, cette architecture nécessite de coupler au lecteur et au badge, deux dispositifs, l'un pour l'émission et l'autre pour la réception. Côté lecteur, le signal de demande d'authentification est émis en basse fréquence (LF - 100KHZ à 150KHZ). Ce choix est justifié par le fait que les circuits de réception existants qui fonctionnent à des fréquences aussi basses, consomment très peu énergie et peuvent donc rester en réception permanente notamment pour le badge qui est plus contraint que le lecteur en terme de taille et d'autonomie. Pour la réponse, le badge exploite à une fréquence plus élevée (HF - 8MHZ à 15MHZ) car elle est moins atténuée par le corps humain que le premier signal en basse fréquence émis par le lecteur et qu'elle rend possible l'utilisation d'une pile de très faible capacité et donc d'encombrement pour être facilement transportée par l'utilisateur. L'inconvénient de cette architecture est qu'elle nécessite, côté lecteur, de nombreux composants pour la réception, l'amplification et l'adaptation du signal HF de réponse et paraît plus complexe en ce sens qu'elle ne suppose pas seulement de juxtaposer un émetteur et un récepteur simple de mise en œuvre.

L'invention propose une solution alternative aux problèmes précédemment évoqués et pour établir des communications bidirectionnelles entre le lecteur et le dispositif portatif dans le but d'améliorer le confort d'utilisation et de sécuriser les transmissions, notamment des codes d'identification.

30 En effet, l'inventeur s'est rendu compte que la transmission par le corps humain, combinée aux moyens de communication radiofréquence RF de la commande à distance, pour le canal de réponse vers le lecteur, permettrait non seulement une communication bidirectionnelle sécurisée mais aussi de garantir que le procédé d'authentification a bien été initié volontairement par le porteur du dispositif portatif et ainsi d'éviter les tentatives de copie et les « attaques par relais », problème typiquement rencontré avec les systèmes d'accès sans mains libres aux véhicules.

Dans les systèmes de contrôle d'accès des bâtiments, un même badge doit permettre à son porteur de passer l'entrée principale du bâtiment puis d'accéder à son bureau. Donc un même badge doit pouvoir être lu par plusieurs lecteurs. Les techniques de « code tournant » ou de « saut de code » utilisées dans les transmissions unidirectionnelles et basées sur une synchronisation parfaite de leurs compteurs, ne permettent pas d'associer un même émetteur à plusieurs récepteurs au risque d'être souvent désynchronisé. En revanche, avec une communication bidirectionnelle, chaque lecteur gère son propre compteur et le dispositif portable utilise la valeur de compteur à usage unique, fournie par le lecteur en même temps que la demande d'identification, pour encrypter son identifiant avant de transmettre les données cryptées en radiofréquence. Il n'y a alors plus de problème de synchronisation. La sécurité est également renforcée par l'utilisation de la transmission par le corps humain pour fournir la valeur de compteur à usage unique au dispositif portable combinée au canal de réponse en radiofréquence pour l'envoi du code d'identification encryptée vers le dispositif fixe.

L'invention réside dans le fait que le dispositif portable comprend en outre un circuit de communication en champ proche capable d'exploiter aussi bien un champ magnétique qu'un champ électrique. Ainsi, le dispositif portable présente l'avantage d'être compatible avec les lecteurs RFID standards de l'art antérieur, exploitant un champ magnétique. Dans ce cas, l'utilisateur doit sortir son dispositif portable de sa poche et le présenter devant le lecteur tout en pressant un bouton ou une combinaison de boutons, pour garantir que le procédé d'authentification a été initié volontairement par le porteur du dispositif portable. Le dispositif portable simule alors le comportement d'un badge RFID standard et transmet son code d'identification vers le lecteur en agissant sur la commutation d'une charge qui atténue le champ magnétique et qui est vu comme une modulation d'amplitude par le lecteur.

Le système selon l'invention comporte, un dispositif fixe de lecture de badge « lecteur » mettant en œuvre un canal de transmission par courant traversant le corps humain pour transmettre un signal de réveil et de demande d'authentification vers un dispositif portable. Le dispositif portable qui comporte aussi des moyens de communication radiofréquence RF pour la fonction de commande à distance, utilise ce canal de transmission existant pour répondre au lecteur.

Selon un autre aspect de l'invention, le dispositif portable comprend une unité de réception en champ proche avec un circuit d'adaptation permettant de détecter soit un champ magnétique via un circuit résonant LC composé d'une inductance et d'un condensateur, soit un champ électrique grâce à une antenne directement imprimée sur le circuit imprimé.

Ainsi, lorsque le dispositif portable est présenté devant un dispositif fixe de lecture de badge RFID de l'art antérieur exploitant uniquement le champ magnétique pour lire l'identifiant, le dispositif portable commutera une charge au circuit résonant LC servant d'antenne qui atténue le champ magnétique émis par le dispositif fixe et qui est vu comme une modulation d'amplitude par son circuit de réception.

- 5 -

Selon un autre aspect de l'invention, le dispositif portatif comprend une unité de transmission radiofréquence vers le dispositif fixe pouvant aussi piloter d'autres équipements comme par exemple la commande d'ouvrants (porte de garage, barrière de parking, volets roulants...) limitée seulement par le nombre de boutons.

5 Selon un autre aspect de l'invention, le dispositif portatif comprend une mémoire EEPROM qui contient les numéros d'identification unique programmés en usine et les valeurs des compteurs de l'algorithme de cryptage par « code tournant » pour les transmissions unidirectionnelles pilotant les autres équipements de commande d'ouvrants associés aux boutons.

10 Selon un autre aspect de l'invention, le dispositif fixe comprend une unité de détection capacitive associée à une plaque de couplage pour, à la fois détecter l'approche ou le toucher de l'utilisateur et pour transmettre par l'intermédiaire de son corps le signal de réveil et d'interrogation généré par un générateur LF vers le dispositif portatif.

15 Selon un autre aspect de l'invention, le dispositif fixe comprend une unité de réception radiofréquence associé à une antenne pour la réception du code d'identification transmis par le dispositif portatif.

20 Selon un autre aspect de l'invention, le dispositif fixe comprend une unité de transmission des numéros d'identification des dispositifs portatifs lus, vers un équipement distant de gestion centralisée de contrôle d'accès. Cette unité de transmission peut être soit filaire, soit sans fils en radiofréquence. Dans le cas d'une liaison sans fils en radiofréquence, l'antenne utilisée pour la réception du code d'identification transmis par le dispositif portatif, sert également pour l'émission des signaux radiofréquences vers l'équipement distant de gestion centralisée.

D'autres caractéristiques et avantages de l'invention ressortiront clairement de la description qui en est faite ci-après, en référence aux dessins annexés dans lesquels :

25 La figure 1 illustre une communication bidirectionnelle entre le dispositif fixe de lecture (1) et le dispositif portatif (2) de l'invention. Dans ce mode de fonctionnement, la communication est initiée lorsque l'utilisateur touche la surface sensitive (102). Le dispositif fixe (1) transmet alors un signal de réveil et d'interrogation vers le dispositif portatif (2), par couplage capacitive à travers le corps de l'utilisateur. L'antenne (202) permet la détection du champ électrique ainsi transmis par l'intermédiaire du corps de l'utilisateur et si une réponse est requise, le dispositif portatif (2) la  
30 transmet avec son identifiant via son antenne (201) en radiofréquence. L'antenne (101) du dispositif fixe (1) reçoit le signal radiofréquence puis l'information est transférée par l'interface de communication (107) vers un équipement distant de gestion centralisée de contrôle d'accès.

35 La figure 2 est un schéma illustrant un système connu d'identification de l'art antérieur, dans lequel le dispositif fixe (3) émet en permanence un champ magnétique modulé, via le circuit résonant LC (301) composé d'une inductance et d'un condensateur. Ce champ magnétique est utilisé pour fournir l'alimentation électrique du dispositif portatif de l'art antérieur (4). Lorsque le

- 6 -

dispositif portatif (4) se trouve dans le champ magnétique, la puce (401) est alimentée et elle transmet aussitôt son code en commutant le circuit (402) qui fait varier la charge inductive qu'elle présente au champ magnétique à travers la bobine (403). L'alimentation électrique (303) du dispositif fixe (3) est généralement fournie par un autre équipement. Après lecture du code  
5 d'identification du dispositif portatif (4), l'interface de communication (306) permet transférer cette information vers un équipement distant de gestion centralisée de contrôle d'accès.

La figure 3 illustre le dispositif portatif (2) de l'invention en mode compatibilité avec un dispositif fixe de lecture de l'art antérieur (3). Dans ce mode de fonctionnement, le dispositif portatif, (2) étant alimenté par sa pile interne, n'exploite pas l'énergie fournie par le champ magnétique. Pour  
10 éviter les copies, l'utilisateur doit presser un des boutons (204) pour autoriser la transmission du code d'identification. La méthode de transmission du dispositif portatif (2) vers le dispositif fixe (3) est identique à celle de l'art antérieur, comme décrit précédemment, par commutation d'une charge qui atténue le champ magnétique et qui est vu comme une modulation d'amplitude par le lecteur.

La figure 4 illustre de manière plus détaillée les dispositifs du système ainsi que leurs  
15 fonctions internes dans un mode de réalisation préférentiel.

Dans ce mode de réalisation, le dispositif fixe (1) comporte une surface sensitive (102) en liaison avec une unité de détection capacitive (103) pour détecter l'approche ou le toucher de l'utilisateur et avec un générateur LF (104) pour transmettre par l'intermédiaire du corps de l'utilisateur, le signal de réveil et d'interrogation vers le dispositif portatif (2).

L'unité centrale (106) est un microcontrôleur comprenant une mémoire RAM, une mémoire ROM contenant le programme informatique et d'autres périphériques tel qu'un générateur de signaux modulés PWM (Pulse Wide Modulation en anglais) soit une modulation de la largeur des impulsions comme source pour le générateur LF (104). La fréquence du générateur (104) peut être de type LF de 125 KHZ à 150KHZ ou HF de 8MHZ à 15MHZ.  
20

L'interface de communication (107) permet de transférer les numéros d'identification des dispositifs portatifs lus, vers un équipement distant de gestion centralisée de contrôle d'accès.  
25

L'unité de réception radiofréquence (108) associé à l'antenne (101) pour la réception du code d'identification transmis par le dispositif portatif (2) peut aussi être de type émetteur + récepteur et assurer ainsi le transfert sans fils en radiofréquence, des identifiants lus vers  
30 l'équipement distant de gestion centralisée de contrôle d'accès. Les émissions radiofréquences doivent être en conformité avec les exigences des réglementations locales. Pour l'Europe, les fréquences autorisées se situent dans les bandes : 433~434MHZ, 868~870MHZ et 2400~2500MHZ.

Le dispositif fixe (1) comprend aussi une alimentation électrique (105) qui peut être soit une alimentation externe fournie par un autre équipement, soit des piles pour un mode de  
35 fonctionnement autonome, notamment lorsque l'interface de communication (107) est une liaison sans fils en radiofréquence.

- 7 -

Le dispositif portatif (2) est de fonctionnement autonome comprenant, pour son alimentation, une pile (207) de taille réduite de manière à être transporté par l'utilisateur.

L'unité centrale (209) du dispositif portatif (2) qui se trouve en mode veille pour réduire au maximum sa consommation est activée soit par une pression sur l'un des boutons (204), soit par  
5 l'unité de réception en champ proche (206) lorsqu'un signal de réveil est détecté.

L'unité centrale (209) est un microcontrôleur comprenant une mémoire RAM et une mémoire ROM contenant le programme informatique et peut aussi intégrer dans la même puce, la mémoire EEPROM (208) pour stocker les numéros d'identifications uniques programmés en usine et les valeurs des compteurs de l'algorithme de cryptage « code tournant » pour les transmissions  
10 unidirectionnelles pilotant les autres équipements comme par exemple les commandes d'ouverture ou de mise en service associées aux boutons (204).

L'unité de réception en champ proche (206) est un circuit intégré d'interface pour transpondeur ne consommant pas plus quelques microampères, connu de l'homme du métier et capable de détecter un champ magnétique via le circuit résonant LC (203) composé d'une  
15 inductance et d'un condensateur. Grâce au circuit d'adaptation (205), l'unité de réception (206) peut également détecter un champ électrique, véhiculé à travers le corps de l'utilisateur, via l'antenne (202) qui peut être directement imprimée sur le circuit imprimé. Les signaux ainsi détectés sont mis en forme et transférés vers l'unité centrale (209) pour analyse. Ces signaux transportent les commandes de réveil, de demande d'authentification et également la valeur d'un compteur propre  
20 au dispositif fixe (1) et à usage unique, pour le cryptage par « code tournant ».

L'unité de transmission radiofréquence (210) et son antenne (201) permettent de transmettre l'identifiant au dispositif fixe (1) et de piloter d'autres équipements pour l'ouverture ou la fermeture de porte de garage, barrière de parking, volets roulants... etc.

L'unité de réception en champ proche (206) étant un circuit intégré d'interface pour  
25 transpondeur, elle comporte un circuit de commutation interne qui peut faire varier la charge inductive qu'elle présente au champ magnétique à travers le circuit résonant LC (203). La modulation d'amplitude ainsi produite, peut être détectée par le circuit de réception (304) du dispositif fixe de l'art antérieur (3) pour en extraire le code d'identification.

Dans ce mode de réalisation, le dispositif fixe (1) met toutes ses fonctions en veille sauf  
30 l'unité de détection capacitive (103) reliée à la surface sensitive (102) et qui analyse périodiquement soit le toucher, soit l'approche de la main de l'utilisateur. Dès que la proximité de la main de l'utilisateur est détectée, l'unité de détection capacitive (103) est désactivée puis le générateur LF (104) génère un signal modulé pour transmettre par l'intermédiaire du corps de l'utilisateur, un signal de réveil et d'interrogation vers le dispositif portatif (2). Dans le même temps, l'unité de réception  
35 radiofréquence (108) est activée et mise en position d'attente de la réponse du dispositif portatif (2) par le canal de transmission radiofréquence. Si la réponse n'est pas reçue, le dispositif fixe (1) émet

- 8 -

à nouveau la commande de réveil en demandant un changement de fréquence de façon à exploiter d'autres sous bandes de fréquences autorisées par les réglementations en vigueur et ainsi d'augmenter les chances d'établir la liaison même en présence de perturbations RF. Si aucune réponse n'est reçue, l'opération est répétée jusqu'au retrait de la main de l'utilisateur ou jusqu'à  
5 atteindre le nombre maximum de tentatives prédéterminé puis le dispositif fixe (1) retourne en mode veille.

Cette méthode permet d'optimiser la durée de réception et ainsi de limiter d'éventuelles latences provoquées par des durées de réception et d'émission fixes. La consommation est ainsi réduite et la durée de vie des piles prolongée, aussi bien pour le dispositif portatif (2) que pour le  
10 dispositif fixe (1) surtout lorsque qu'il est utilisé en mode autonome.

La commande de réveil est accompagnée de la valeur d'un compteur, propre à chaque dispositif fixe (1) et à usage unique, pour générer un « code tournant » qui change à chaque nouvel échange de données. Le dispositif portatif (2) utilise cette valeur pour encrypter son code d'identification avant de le transmettre.

15 L'incrémentation du compteur n'est pas linéaire de façon à rendre le plus complexe possible l'analyse et le déchiffrement des données échangées.

La fonction de commande à distance d'autres équipements est en revanche basée sur une technique de « code tournant » existant et adaptée pour les transmissions unidirectionnelles. L'identifiant pour cette fonction peut être différent de celui utilisé pour le contrôle d'accès pour plus  
20 de sécurité.

Toutefois l'appairage du dispositif portatif (2) avec un récepteur de commande d'ouvrants peut utiliser la transmission par le corps humain pour sécuriser la transmission de données non cryptées durant cette phase.

Ce fonctionnement est différent des systèmes connus de l'art antérieur en ce sens que, tout  
25 en conservant la compatibilité avec les équipements existants, il est proposé ici une méthode d'identification et d'accès sans clé, sécurisé, simple et qui permet en mutualisant certains composants, de diminuer l'encombrement et le coût de fabrication des dispositifs.

En effet, la présente invention apporte une solution simple et utilisable dans de très nombreuses circonstances pour résoudre les problèmes précités.

30 Bien entendu, l'invention n'est pas limitée au mode de réalisation décrit et représenté qui n'a été donné qu'à titre d'exemple. L'invention peut en outre être utilisée pour d'autres procédés d'identification ou d'autorisation. Par exemple, l'invention peut s'appliquer à un procédé de mise en service et de mise hors service d'équipements qui nécessitent une sécurisation par l'identification des personnes autorisées. Le dispositif fixe (1) peut aussi être combiné à un clavier à code tactile  
35 (touches capacitives) en mutualisant une fois de plus certains composants.

## REVENDICATIONS

1) Système d'identification automatique par le toucher permettant de donner un accès sans clé  
5 à un espace ou à un objet sans l'utilisation d'une clé physique, comportant au moins un dispositif  
fixe (1) de type lecteur de badge et un dispositif portable (2) de type badge intégré à une  
télécommande, caractérisé en ce qu'il comporte des moyens mettant en œuvre un canal de  
communication en champ proche exploitant aussi bien un champ magnétique qu'un champ  
électrique et un canal de communication radiofréquence, pour établir des communications  
10 bidirectionnelles entre le dispositif fixe (1) et le dispositif portable (2).

2) Système d'identification automatique par le toucher et d'accès sans clé selon la  
revendication 1 caractérisé en ce que le dispositif fixe (1) comporte un élément de couplage  
capacitif (102) relié d'une part, sous la forme d'une surface sensible, à l'unité de détection  
capacitive (103) pour détecter le toucher de l'utilisateur et d'autre part, comme antenne, à l'unité  
15 d'émission basse fréquence (104) pour mettre en œuvre le canal de transmission en champ proche  
traversant le corps humain, destinés à activer le dispositif portable (2) par l'envoi d'un signal de réveil  
et de demande d'authentification et surtout, fournir de manière sécurisée la valeur d'un compteur  
interne du dispositif fixe (1), générée de manière non linéaire et à usage unique pour l'algorithme de  
« code tournant ».

20 3) Système d'identification automatique par le toucher et d'accès sans clé selon la  
revendication 1 ou la revendication 2 caractérisé en ce que le dispositif fixe (1) comporte des  
moyens (101, 108) mettant en œuvre un canal de réception ou d'émission/réception par  
radiofréquence, destinés à recevoir, en réponse à sa demande d'authentification, le code  
d'identification encryptée du dispositif portable (2).

25 4) Système d'identification automatique par le toucher et d'accès sans clé selon l'une  
quelconque des revendications précédentes caractérisé en ce que le dispositif fixe (1) qui comporte  
les moyens (101, 108) et qui sont utilisés pour la réception du code d'identification transmis par le  
dispositif portable (2), servent également à établir une liaison sans fils entre le dispositif fixe (1) et un  
équipement distant de gestion centralisée de contrôle d'accès, pour l'émission des codes  
30 d'identification lus.

5) Système d'identification automatique par le toucher et d'accès sans clé selon l'une  
quelconque des revendications précédentes caractérisé en ce que le dispositif portable (2) comporte  
des moyens (202, 205, 206) mettant en œuvre un canal de réception en champ proche pour  
détecter le champ électrique véhiculé à travers le corps de l'utilisateur.

35 6) Système d'identification automatique par le toucher et d'accès sans clé selon l'une  
quelconque des revendications précédentes caractérisé en ce que le dispositif portable (2) comporte  
des moyens (201, 210) mettant en œuvre un canal de transmission radiofréquence destiné à  
transmettre son code d'identification vers le dispositif fixe (1).

- 10 -

7) Système d'identification automatique par le toucher et d'accès sans clé selon l'une quelconque des revendications précédentes caractérisé en ce que le dispositif portatif (2) comporte des moyens (203, 205, 206) mettant en œuvre un canal de communication en champ proche capable de détecter le champ magnétique émis par un dispositif fixe de lecture de l'art antérieur (3) et de lui transmettre son code d'identification en commutant une charge au circuit résonant LC (203) qui atténue le champ magnétique pour produire une modulation d'amplitude.

1/2

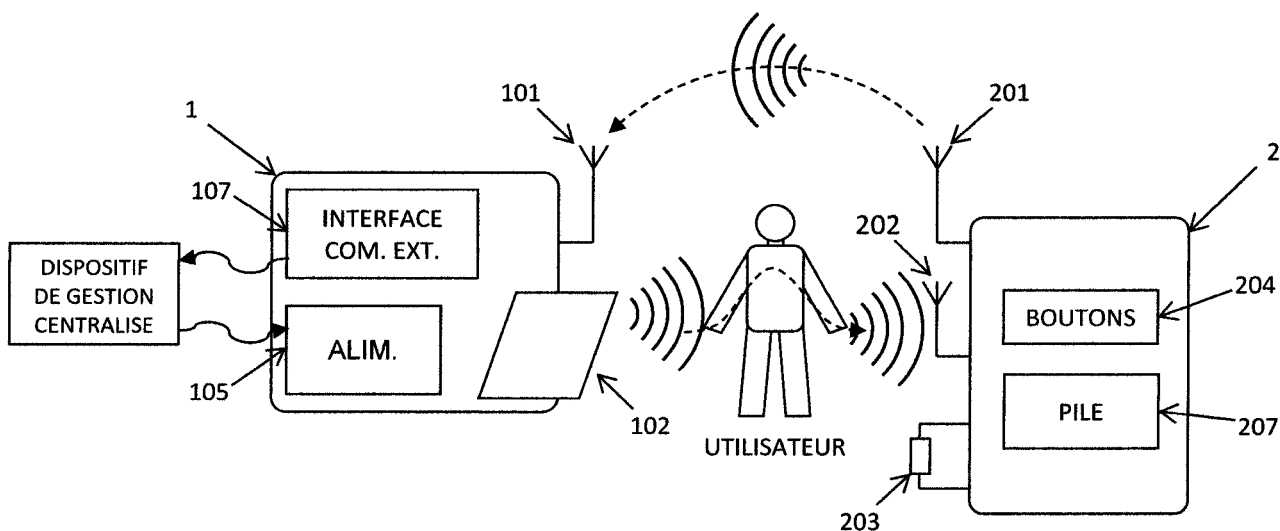


FIG. 1

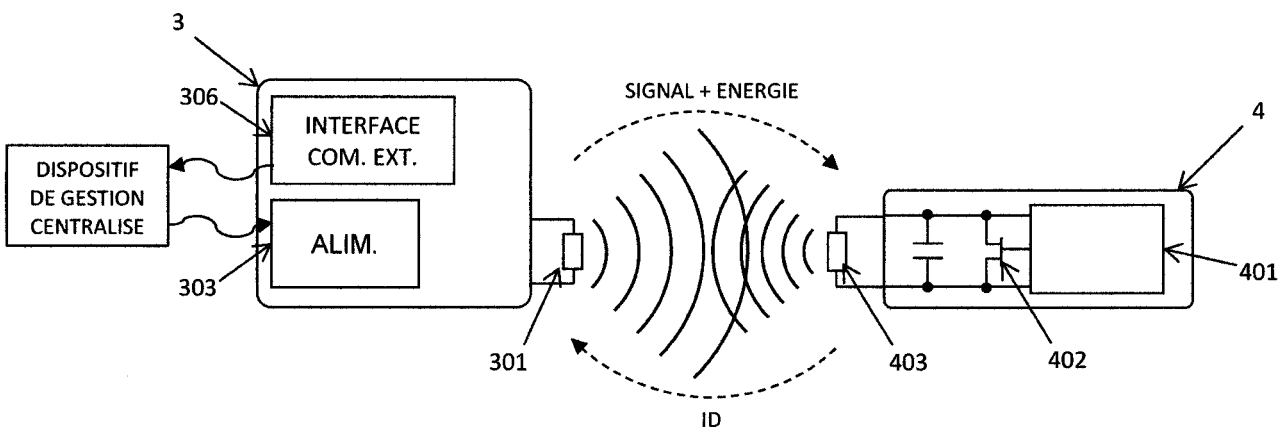


FIG. 2

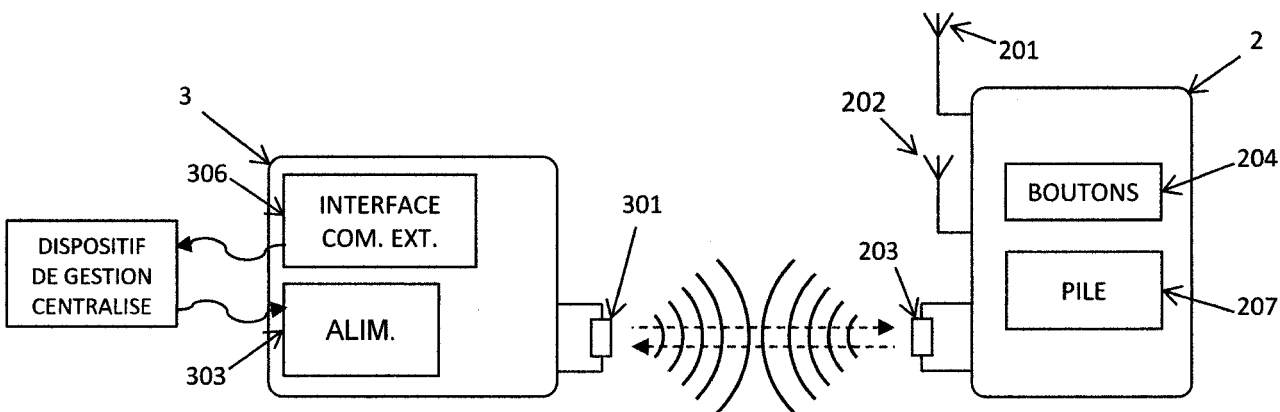


FIG. 3

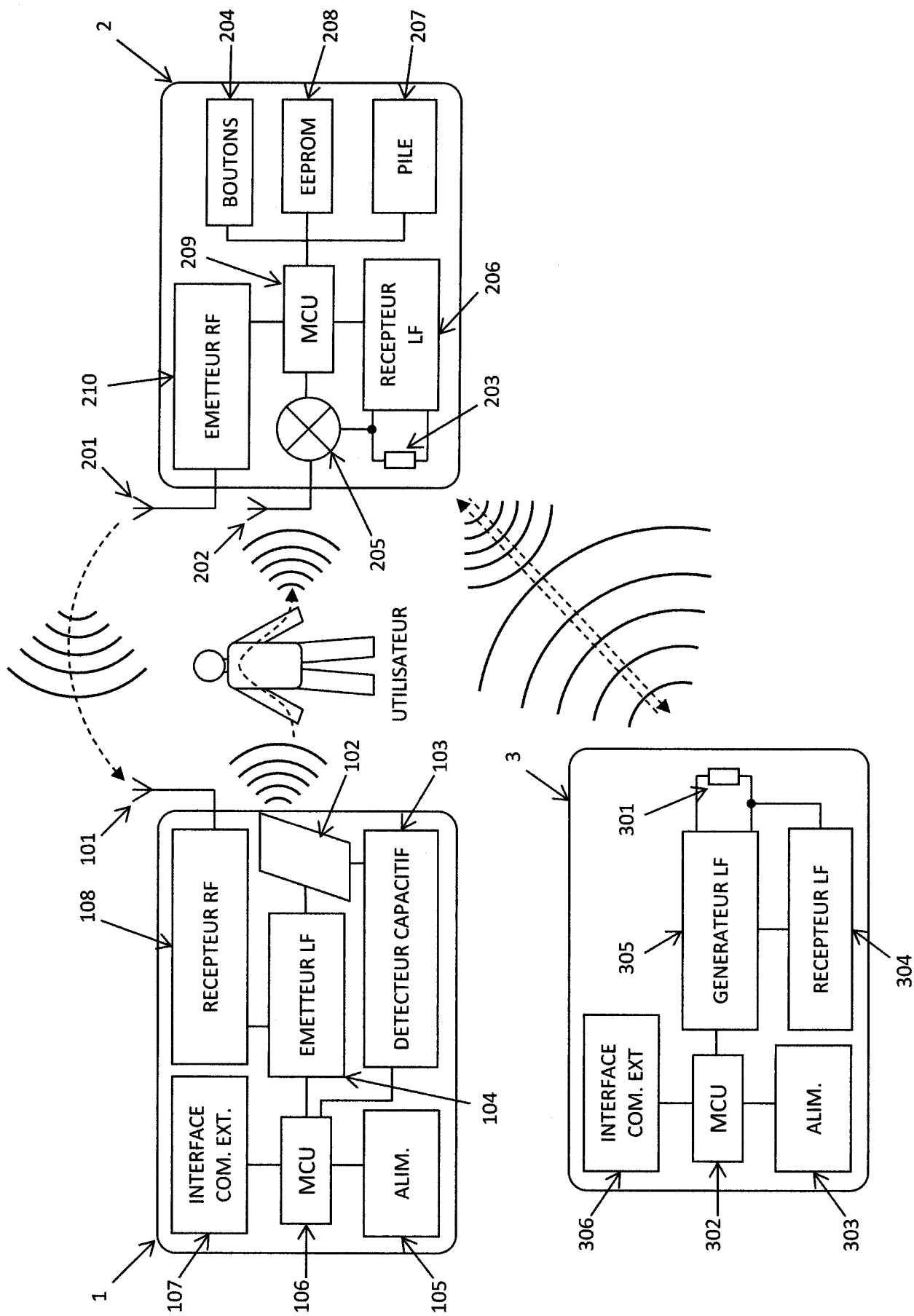


FIG. 4



**RAPPORT DE RECHERCHE  
PRÉLIMINAIRE**

établi sur la base des dernières revendications  
déposées avant le commencement de la recherche

N° d'enregistrement  
national

FA 798472  
FR 1401315

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	WO 2005/109699 A1 (VALEO SECURITE HABITACLE SAS [FR]; MUSAT CIPRIAN [FR]; COURJAULT GILLÉ) 17 novembre 2005 (2005-11-17) * alinéas [0049] - [0051] * * alinéas [0059] - [0068] * * alinéas [0079] - [0085] * * alinéas [0098] - [0143] * * figures 1-5 *	1-7	H04L9/32 H04W12/08
X	FR 2 942 755 A1 (CONTINENTAL AUTOMOTIVE FRANCE [FR]) 10 septembre 2010 (2010-09-10) * page 6, ligne 16 - page 9, ligne 36 * * figures 1-4d *	1-7	
X	EP 2 582 113 A1 (GEMALTO SA [FR]) 17 avril 2013 (2013-04-17) * alinéas [0003], [0014] - [0022] * * alinéas [0025] - [0027] * * figures 1-5 *	1-7	
X	EP 1 274 038 A1 (TEXAS INSTRUMENTS DEUTSCHLAND [DE]) 8 janvier 2003 (2003-01-08) * alinéas [0010] - [0015] * * figures 1,2 *	1-7	B60R H04W H04B G07C H04L
A	FR 2 992 442 A1 (FRANCE TELECOM [FR]) 27 décembre 2013 (2013-12-27) * page 7, ligne 4 - page 12, ligne 29 * * figures 1-3 *	1-7	
Date d'achèvement de la recherche		Examineur	
30 janvier 2015		Ghomrasseni, Z	
CATÉGORIE DES DOCUMENTS CITÉS		T : théorie ou principe à la base de l'invention	
X : particulièrement pertinent à lui seul		E : document de brevet bénéficiant d'une date antérieure	
Y : particulièrement pertinent en combinaison avec un		à la date de dépôt et qui n'a été publié qu'à cette date	
autre document de la même catégorie		de dépôt ou qu'à une date postérieure.	
A : arrière-plan technologique		D : cité dans la demande	
O : divulgation non-écrite		L : cité pour d'autres raisons	
P : document intercalaire		& : membre de la même famille, document correspondant	

2

EPO FORM 1503 12.99 (P04C14)

**ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE  
RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1401315 FA 798472**

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.

Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du **30-01-2015**

Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 2005109699	A1	17-11-2005	FR 2869859 A1 WO 2005109699 A1	11-11-2005 17-11-2005
-----				
FR 2942755	A1	10-09-2010	AUCUN	
-----				
EP 2582113	A1	17-04-2013	EP 2582113 A1 EP 2767061 A1 WO 2013053923 A1	17-04-2013 20-08-2014 18-04-2013
-----				
EP 1274038	A1	08-01-2003	DE 10132031 A1 EP 1274038 A1 JP 2003097112 A US 2003025588 A1	23-01-2003 08-01-2003 03-04-2003 06-02-2003
-----				
FR 2992442	A1	27-12-2013	FR 2992442 A1 WO 2014001704 A1	27-12-2013 03-01-2014
-----				