(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 986 686**

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **12 00308**

(51) Int Cl[8] : ***H 04 W 12/06*** *(2013.01)*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 02.02.12.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 09.08.13 Bulletin 13/32.

(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 :**

(71) **Demandeur(s) :** *CONTINENTAL AUTOMOTIVE FRANCE* — FR et *CONTINENTAL AUTOMOTIVE GMBH* — DE.

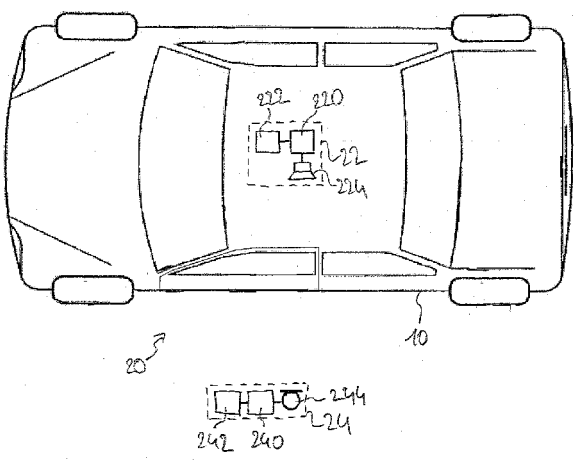
(72) **Inventeur(s) :** JANSSEUNE LUC.

(73) **Titulaire(s) :** CONTINENTAL AUTOMOTIVE FRANCE, CONTINENTAL AUTOMOTIVE GMBH.

(74) **Mandataire(s) :** CONTINENTAL AUTOMOTIVE FRANCE Société par actions simplifiée.

(54) PROCEDE ET SYSTEME D'AUTHENTIFICATION D'UN DISPOSITIF DE COMMANDE VIS-A-VIS D'UNE UNITE CENTRALE D'UN VEHICULE.

(57) La présente invention concerne un procédé (50) d'authentification d'un dispositif de commande (24) vis-à-vis d'une unité centrale (22) d'un véhicule (10), l'authentification dudit dispositif de commande s'effectuant au cours d'une session d'authentification en échangeant des données d'authentification entre ledit dispositif de commande et ladite unité centrale sous la forme de signaux radioélectriques. En outre, le procédé (50) d'authentification comporte l'évaluation de la présence du dispositif de commande (24) à l'intérieur du véhicule (10) par l'émission, à l'intérieur dudit véhicule, d'un signal acoustique par l'unité centrale (22), ledit dispositif de commande (24) ne pouvant être considéré comme étant à l'intérieur du véhicule (10) que lorsque ledit dispositif de commande (24) a détecté ledit signal acoustique. L'invention concerne également un système (20) d'authentification et un véhicule (10) comportant un tel système (20) d'authentification.



FR 2 986 686 - A1

La présente invention appartient au domaine de la sécurisation de l'accès à des ressources, et concerne plus particulièrement un procédé et un système d'authentification d'un dispositif de commande vis-à-vis d'une unité centrale d'un véhicule, par exemple d'un véhicule automobile.

Dans le cas d'un véhicule automobile, le dispositif de commande correspond à une clé dudit véhicule automobile, et l'authentification est préalable à une action effectuée par l'unité centrale, telle que le démarrage dudit véhicule automobile.

De nos jours, de plus en plus de fonctionnalités sont intégrées dans les téléphones portables. Il est également envisagé d'intégrer dans un téléphone portable une clé de véhicule automobile. La clé pourrait alors se présenter sous la forme d'un logiciel pouvant être téléchargé dans le téléphone portable, et l'authentification vis-à-vis du véhicule automobile se ferait en utilisant des moyens de communication sans fil dudit téléphone portable.

Toutefois, les moyens de communication sans fil des téléphones portables actuels (GPRS, UMTS, WiFi, Bluetooth, etc.) ont des portées qui sont généralement supérieures à dix mètres. Or, on comprend qu'il n'est pas souhaitable que le démarrage du véhicule automobile puisse être rendu possible par la simple présence du dispositif de commande à une distance de dix mètres ou plus dudit véhicule automobile.

Par conséquent, d'autres moyens doivent être mis en œuvre pour assurer que le téléphone portable intégrant la clé du véhicule automobile se trouve à proximité immédiate du véhicule automobile.

Pour autoriser le démarrage, il faut au moins assurer que le téléphone portable se trouve à l'intérieur du véhicule automobile.

Il faut également pouvoir déterminer si le téléphone portable se trouve à l'intérieur du véhicule automobile dans le cas d'une authentification visant à autoriser le verrouillage des portes du véhicule automobile, afin de refuser le verrouillage si le téléphone portable est à l'intérieur du véhicule automobile.

La présente invention a pour objectif de proposer une solution qui permette d'authentifier un dispositif de commande vis-à-vis d'une unité centrale d'un véhicule, tout en évaluant la proximité dudit dispositif de commande par rapport à ladite unité centrale.

A cet effet, l'invention concerne, selon un premier aspect, un procédé d'authentification d'un dispositif de commande vis-à-vis d'une unité centrale d'un véhicule, l'authentification dudit dispositif de commande s'effectuant au cours d'une session d'authentification en échangeant des données d'authentification entre ledit dispositif de commande et ladite unité centrale sous la forme de signaux radioélectriques. En outre, le

procédé d'authentification comporte l'évaluation de la présence du dispositif de commande à l'intérieur du véhicule par l'émission, à l'intérieur dudit véhicule, d'un signal acoustique par l'unité centrale, ledit dispositif de commande ne pouvant être considéré comme étant à l'intérieur du véhicule que lorsque ledit dispositif de commande a détecté ledit signal acoustique.

On comprend qu'un signal acoustique émis à l'intérieur du véhicule pourra difficilement être détecté depuis l'extérieur dudit véhicule, du fait d'une absorption par des parois dudit véhicule et/ou du fait de nuisances sonores importantes à l'extérieur dudit véhicule. Si nécessaire, le signal acoustique peut en outre être calibré, en fréquences et en puissance, de sorte à assurer qu'il ne puisse pas être détecté depuis l'extérieur du véhicule.

Par conséquent, en évaluant la présence du dispositif de commande lors d'une session d'authentification avec l'unité centrale, il sera possible de conditionner l'exécution de l'action envisagée non seulement à la réussite de l'authentification, mais également à la présence ou non du dispositif de commande à l'intérieur du véhicule.

Si l'action envisagée est le démarrage du véhicule, ledit démarrage ne doit être autorisé que si le dispositif de commande est considéré comme étant à l'intérieur du véhicule (sous réserve d'une authentification réussie). Si l'action est envisagée est le verrouillage des portes du véhicule, ledit verrouillage ne doit être autorisé que si le dispositif de commande est considéré comme étant à l'extérieur du véhicule (sous réserve d'une authentification réussie).

De plus, un procédé d'authentification selon l'invention est plus robuste aux attaques par relais (« relay attacks » dans la littérature anglo-saxonne) que les procédés d'authentification de l'art antérieur. Il est en effet plus difficile d'effectuer une attaque par relais car il faut non seulement relayer les signaux radioélectriques, mais également le signal acoustique, émis à l'intérieur du véhicule qui est de surcroît difficilement détectable depuis l'extérieur du véhicule.

En outre, on comprend que les téléphones portables actuels sont tous équipés d'un microphone qui peut être mis en œuvre pour la détection d'un signal acoustique de fréquences comprises dans le spectre des sons audibles. Ainsi, si le dispositif de commande est un téléphone portable, le procédé d'authentification peut être mis en œuvre par une simple mise à jour logicielle dudit téléphone portable. On comprend également que les véhicules actuels, notamment les véhicules automobiles, sont généralement équipés de haut-parleurs qui peuvent être mis en œuvre pour l'émission d'un signal acoustique de fréquences comprises dans le spectre des sons audibles.

Suivant des modes particuliers de mise en œuvre, le procédé d'authentification comporte l'une ou plusieurs des caractéristiques suivantes, prises isolément ou suivant toutes les combinaisons techniquement possibles.

Dans un mode particulier de mise en œuvre, une partie des données d'authentification formées par l'unité centrale sont émises, de ladite unité centrale vers le dispositif de commande, par l'intermédiaire du signal acoustique.

De telles dispositions permettent, de manière particulièrement simple, d'assurer que l'authentification ne pourra être réussie que si le dispositif de commande détecte le signal acoustique.

Dans un mode particulier de mise en œuvre, le procédé d'authentification comporte des étapes :

- d'émission, par l'unité centrale, d'un signal radioélectrique à destination du dispositif de commande, dit « signal de requête UC », comportant des données d'authentification,
- d'émission, par le dispositif de commande et suite à la réception du signal de requête UC et du signal acoustique, d'un signal radioélectrique à destination de l'unité centrale, dit « signal de réponse », comportant des données d'authentification déterminées en fonction des données d'authentification incluses dans le signal de requête UC et dans le signal acoustique.

De telles dispositions permettent d'assurer, au niveau de l'unité centrale, que c'est bien le même dispositif de commande qui a reçu à la fois le signal de requête UC et le signal acoustique. En effet, dans le cas contraire, les données d'authentification incluses dans le signal de réponse ne pourront pas correspondre aux données d'authentification attendues par l'unité centrale, et l'authentification échouera.

Dans un mode particulier de mise en œuvre :

- le procédé d'authentification comporte une étape d'émission, par le dispositif de commande, d'un signal radioélectrique à destination de l'unité centrale dit « signal de requête DC », comportant des données de vérification,
- le signal acoustique comporte des données de vérification déterminées en fonction des données de vérification incluses dans le signal de requête DC,
- le procédé d'authentification comporte une étape de comparaison, par le dispositif de commande, des données de vérification reçues dans le signal acoustique avec les données de vérification émises dans le signal de requête DC.

Dans un mode particulier de mise en œuvre, les données de vérification incluses dans le signal de requête DC se présentent sous la forme d'une trame audionumérique, et le signal acoustique correspond à la traduction analogique de ladite trame audionumérique.

De telles dispositions permettent d'évaluer la présence du dispositif de commande à l'intérieur du véhicule y compris dans le cas d'une unité centrale ne pouvant pas envoyer des données d'authentification qu'elles a elle-même formées sous la forme d'un signal acoustique. C'est par exemple le cas si le seul moyen d'émission acoustique est un haut-parleur d'un module de téléphonie mains-libres Bluetooth, un tel haut-parleur ne pouvant généralement diffuser que les trames audionumériques reçues sous la forme d'un signal radioélectrique Bluetooth. Dans ce cas, le dispositif de commande peut envoyer une trame audionumérique qu'il a lui-même formée, et vérifier que le signal acoustique reçu correspond bien à la traduction analogique de ladite trame audionumérique. Si c'est le cas, le dispositif de commande pourra considérer qu'il se trouve à l'intérieur du véhicule.

Dans un mode particulier de mise en œuvre, si les données de vérification reçues dans le signal acoustique ont bien été déterminées à partir des données de vérification incluses dans le signal de requête DC, le procédé d'authentification comporte une étape d'émission, par le dispositif de commande, d'un signal radioélectrique à destination de l'unité centrale, dit « signal de réponse », comportant des données d'authentification déterminées en fonction de données d'authentification incluses dans un signal radioélectrique préalablement reçu de l'unité centrale.

Dans un mode particulier de mise en œuvre, le procédé d'authentification comporte une étape d'émission, par l'unité centrale, d'un signal radioélectrique à destination du dispositif de commande, dit « signal de réveil », le signal de réveil étant émis avant d'émettre le signal acoustique.

Selon un second aspect, l'invention concerne un système d'authentification comportant un dispositif de commande à authentifier vis-à-vis d'une unité centrale d'un véhicule, ledit dispositif de commande et ladite unité centrale comportant chacun :

- un module d'authentification adapté à former des données d'authentification,
- un module de communication sans fil adapté à émettre et recevoir des signaux radioélectriques comportant des données d'authentification.

En outre, le système d'authentification est configuré pour évaluer la présence du dispositif de commande à l'intérieur du véhicule par l'émission, à l'intérieur dudit véhicule, d'un signal acoustique par un module d'émission acoustique de l'unité centrale, le dispositif de commande ne pouvant être considéré comme étant à l'intérieur du

véhicule que lorsque le signal acoustique a été détecté par le dispositif de commande équipé d'un module de réception acoustique.

Dans un mode particulier de réalisation, l'unité centrale est adaptée à émettre des données d'authentification formées par le module d'authentification de ladite unité centrale par l'intermédiaire du module d'émission acoustique et/ou l'unité centrale est adaptée à émettre un signal acoustique correspondant à une trame audionumérique reçue par l'intermédiaire du module de communication sans fil de ladite unité centrale, sans passer par le module d'authentification de ladite unité centrale.

Selon un troisième aspect, l'invention concerne un véhicule, tel qu'un véhicule automobile, comportant un système d'authentification selon l'un quelconque des modes de réalisation de l'invention.

L'invention sera mieux comprise à la lecture de la description suivante, donnée à titre d'exemple nullement limitatif, et faite en se référant aux figures qui représentent :

- Figure 1 : une représentation schématique d'un exemple de système d'authentification, selon l'invention,
- Figure 2 : une représentation schématique d'un autre exemple de système d'authentification, selon l'invention,
- Figure 3 : un diagramme représentant les principales étapes d'un exemple de procédé d'authentification, selon l'invention,
- Figure 4 : un diagramme représentant les principales étapes d'un autre exemple de procédé d'authentification, selon l'invention.

Dans ces figures, des références identiques d'une figure à une autre désignent des éléments identiques ou analogues. Pour des raisons de clarté, les éléments représentés ne sont pas à l'échelle, sauf mention contraire.

La présente invention concerne l'authentification d'un dispositif de commande 24 vis-à-vis d'une unité centrale 22 d'un véhicule, tel qu'un véhicule automobile 10.

De manière générale, cette authentification vise à autoriser une action à effectuer par l'unité centrale 22.

Par exemple, l'authentification vise à autoriser / refuser le démarrage du véhicule automobile 10, ou à autoriser / refuser le verrouillage de portes dudit véhicule automobile. Dans ces deux cas, il faut vérifier si le dispositif de commande 24 se trouve à l'intérieur du véhicule automobile 10 :

- pour n'autoriser le démarrage du véhicule automobile 10 que lorsque le dispositif de commande 24 se trouve à l'intérieur dudit véhicule automobile,

- pour n'autoriser le verrouillage des portes du véhicule automobile 10 que lorsque le dispositif de commande 24 se trouve à l'extérieur dudit véhicule automobile.

Dans la suite de la description, on se place de manière nullement limitative dans le cas d'une authentification en vue d'autoriser / refuser le démarrage du véhicule automobile 10. Par conséquent, le démarrage du véhicule automobile ne doit être autorisé que lorsque le dispositif de commande 24 se trouve à l'intérieur du véhicule automobile 10.

La figure 1 représente de manière schématique un exemple de système 20 d'authentification.

Le système 20 d'authentification comporte une unité centrale 22, installée dans le véhicule automobile 10, et un dispositif de commande 24 correspondant à une clé du véhicule automobile 10. Ledit dispositif de commande 24 est par exemple intégré dans un téléphone portable.

L'unité centrale 22 comporte un module d'authentification 220, adapté à former des données d'authentification.

Le module d'authentification 220 de l'unité centrale 22 comporte par exemple un processeur et une mémoire électronique dans laquelle est mémorisé un produit programme d'ordinateur, sous la forme d'un ensemble d'instructions de code de programme à exécuter par le processeur. Dans une variante, le module d'authentification 220 de l'unité centrale 22 comporte des circuits logiques programmables, de type FPGA, PLD, etc., et/ou circuits intégrés spécialisés (ASIC).

Le module d'authentification 220 de l'unité centrale 22 est connecté à un module de communication sans fil 222 et à un module d'émission acoustique 224.

Le module de communication sans fil 222 est adapté à émettre et à recevoir des signaux radioélectriques. Par « signal radioélectrique », on entend une onde électromagnétique dont les fréquences sont comprises dans le spectre traditionnel radiofréquence (quelques hertz à plusieurs centaines de gigahertz) ou dans des bandes de fréquences voisines (y compris infrarouge).

Dans la suite de la description, on se place de manière non limitative dans le cas où le module de communication sans fil de l'unité centrale 22 est un module Bluetooth. Rien n'exclut, suivant d'autres exemples, de considérer d'autres moyens de communication sans fil (GPRS, UMTS, WiFi, etc.).

Le module d'émission acoustique 224 est adapté à émettre des signaux acoustiques. Par « signal acoustique », on entend une onde mécanique dont les fréquences sont comprises dans le spectre traditionnel des sons audibles (de l'ordre de 20 hertz à 20 kilohertz) ou dans des bandes de fréquences voisines (y compris

ultrasonores). Le module d'émission acoustique 224 est par exemple un haut-parleur adapté à émettre des signaux acoustiques de fréquences comprises dans le spectre des sons audibles.

Le module d'authentification 220, le module Bluetooth 222 et le haut-parleur 224 de l'unité centrale 22 forment un ensemble de moyens configurés de façon logicielle (produit programme d'ordinateur spécifique) et/ou matérielle (FPGA, PLD, ASIC, etc.) pour mettre en œuvre les différentes étapes d'un procédé 50 d'authentification devant être exécutées par l'unité centrale 22.

Le dispositif de commande 24 comporte un module d'authentification 240 adapté à former des données d'authentification.

Le module d'authentification 240 du dispositif de commande 24 comporte par exemple un processeur et une mémoire électronique dans laquelle est mémorisé un produit programme d'ordinateur, sous la forme d'un ensemble d'instructions de code de programme à exécuter par le processeur. Dans une variante, le module d'authentification 240 du dispositif de commande 24 comporte des circuits logiques programmables, de type FPGA, PLD, etc., et/ou circuits intégrés spécialisés (ASIC).

Le module d'authentification 240 du dispositif de commande 24 est connecté à un module de communication sans fil 242 et à un module de réception acoustique 244.

Le module de communication sans fil 242 du dispositif de commande 24 est adapté à émettre et à recevoir des signaux radioélectriques.

En outre, ledit module de communication sans fil du dispositif de commande 24 est compatible avec le module de communication sans fil 222 de l'unité centrale 22. En d'autres termes, le module de communication sans fil 242 du dispositif de commande 24 est, dans l'exemple considéré ci-après, un module Bluetooth.

Le module de réception acoustique 244 du dispositif de commande 24 est adapté à recevoir des signaux acoustiques.

En outre, ledit module de réception acoustique 244 est compatible avec le module d'émission acoustique 224 de l'unité centrale 22, c'est-à-dire qu'il est adapté à recevoir les signaux acoustiques émis par ledit module d'émission acoustique. Dans le cas de signaux acoustiques de fréquences comprises dans le spectre des sons audibles, le module de réception acoustique 244 est par exemple un microphone du téléphone portable dans lequel le dispositif de commande 24 est intégré.

Le module d'authentification 240, le module Bluetooth 242 et le microphone 244 du dispositif de commande 24 forment un ensemble de moyens configurés de façon logicielle (produit programme d'ordinateur spécifique) et/ou matérielle (FPGA, PLD, ASIC, etc.) pour mettre en œuvre les différentes étapes d'un procédé 50 d'authentification devant être exécutées par le dispositif de commande 24.

Dans l'exemple illustré par la figure 1, le module d'authentification 220 de l'unité centrale 22 est connecté à la fois au module Bluetooth 222 et au haut-parleur 224. Par conséquent, les données d'authentification formées par ledit module d'authentification de l'unité centrale 22 peuvent être émises, à destination du dispositif de commande 24, sous la forme de signaux radioélectriques et/ou sous la forme de signaux acoustiques.

La figure 2 représente une variante de réalisation d'un système 20 d'authentification.

Le système 20 d'authentification illustré par la figure 2 reprend les mêmes éléments que ceux décrits en référence au système 20 d'authentification illustré par la figure 2.

Toutefois, dans le système 20 d'authentification illustré par la figure 2, le module d'authentification 220 n'est pas connecté au haut-parleur 224. Par contre, le module Bluetooth 222 est connecté au haut-parleur 224 et forme avec ce dernier un module de téléphonie mains-libres Bluetooth. Dans un tel module de téléphonie mains-libres Bluetooth, le haut-parleur 224 ne peut généralement diffuser que des trames audionumériques qu'il reçoit sous la forme d'un signal radioélectrique Bluetooth. Par conséquent, le module d'authentification 220 de l'unité centrale 22 ne peut pas émettre des données d'authentification qu'il a lui-même formées sous la forme de signaux acoustiques. De telles données d'authentification, formées par le module d'authentification 220 de l'unité centrale 22, ne peuvent être émises que sous la forme de signaux radioélectriques.

De manière générale, l'authentification du dispositif de commande 24 vis-à-vis de l'unité centrale 22 du véhicule automobile 10 d'un véhicule s'effectue au cours d'une session d'authentification. Au cours de la session d'authentification, des données d'authentification sont échangées entre le dispositif de commande 24 et l'unité centrale 22 sous la forme de signaux radioélectriques émis / reçus par les modules Bluetooth 242, 222 respectifs desdits dispositif de commande 24 et unité centrale 22.

En outre, un procédé 50 d'authentification selon l'invention comporte l'évaluation de la présence du dispositif de commande 24 à l'intérieur du véhicule automobile 10.

Cette évaluation s'effectue par l'émission, à l'intérieur dudit véhicule automobile par l'unité centrale 22, d'un signal acoustique à destination du dispositif de commande 24. Ledit dispositif de commande ne peut être considéré comme étant à l'intérieur du véhicule que si ledit dispositif de commande détecte ledit signal acoustique.

Par « détecter le signal acoustique », on entend déterminer qu'il s'agit d'un signal acoustique émis par l'unité centrale et/ou extraire sans erreur des données, telles

que des données d'authentification ou autre, éventuellement incluses dans ledit signal acoustique.

Il est à noter que la mise en forme des données d'authentification (cryptage, hachage, etc.) sort du cadre de l'invention et peut mettre en œuvre tout algorithme de mise en forme de données d'authentification connu. Toutefois, l'authentification doit s'accompagner d'une évaluation de la présence du dispositif de commande 24 à l'intérieur du véhicule automobile 10.

La figure 3 représente un exemple de mise en œuvre d'un procédé 50 d'authentification d'un dispositif de commande 24 vis-à-vis d'une unité centrale 22 d'un véhicule automobile 10.

Tel qu'illustré par la figure 3, le procédé 50 d'authentification comporte une étape 52 d'émission, par l'unité centrale 22, d'un signal radioélectrique à destination du dispositif de commande 24, dit « signal de requête UC ». De préférence, le signal de requête UC comporte des données d'authentification.

Le procédé 50 d'authentification comporte également une étape 56 d'émission, par l'unité centrale 22, d'un signal acoustique à destination du dispositif de commande 24.

Dans un mode particulier de mise en œuvre, le signal acoustique est émis après l'émission du signal de requête UC. Ainsi, le signal de requête UC peut être utilisé comme signal de réveil, à la suite de la réception duquel le dispositif de commande 24 s'attend à recevoir un signal acoustique. Par conséquent, le microphone 244 du dispositif de commande 24 peut, par défaut, être désactivé, et n'être activé qu'à partir de la réception, par ledit dispositif de commande 24, dudit signal de requête UC.

Dans un mode préféré de mise en œuvre, une partie des données d'authentification formées par le module d'authentification 220 de ladite unité centrale sont émises par l'intermédiaire du signal acoustique. Il est à noter que, dans ce cas, le procédé 50 d'authentification doit être mis en œuvre par un système 20 d'authentification du type décrit en référence à la figure 1.

De la sorte, on assure de manière particulièrement simple que l'authentification du dispositif de commande 24 ne peut réussir que si le signal acoustique est détecté par ledit dispositif de commande 24.

En effet, si le signal acoustique n'est pas détecté par le dispositif de commande 24, les données d'authentification incluses dans ledit signal acoustique seront perdues. Alors, l'authentification ne pourra pas aboutir et le démarrage du véhicule automobile 10 sera refusé par l'unité centrale 22.

Le procédé 50 d'authentification illustré par la figure 3 comporte une étape 58 d'émission, par le dispositif de commande 24 et suite à la réception du signal de

requête UC et du signal acoustique, d'un signal radioélectrique à destination de l'unité centrale 22, dit « signal de réponse ». Le signal de réponse comporte des données d'authentification.

Dans un mode préféré de mise en œuvre, les données d'authentification incluses dans le signal de réponse sont déterminées, par le module d'authentification 240 du dispositif de commande 24, en fonction des données d'authentification incluses dans le signal de requête UC et dans le signal acoustique.

Un tel mode de mise en œuvre est avantageux en ce qu'il permet d'assurer, au niveau de l'unité centrale 22, que c'est bien un seul et même dispositif de commande 24 qui a reçu à la fois le signal de requête UC et le signal acoustique.

La figure 4 représente un exemple de procédé 50 d'authentification adapté à une mise en œuvre par un système 20 d'authentification tel qu'illustré par la figure 2 (c'est-à-dire dans lequel des données d'authentification formées par le module d'authentification 220 de l'unité centrale 22 ne peuvent émises que sous la forme de signaux radioélectriques).

Tel qu'illustré par la figure 4, le procédé 50 d'authentification comporte une étape 54 d'émission, par le dispositif de commande 24, d'un signal radioélectrique à destination de l'unité centrale dit « signal de requête DC », comportant des données de vérification.

En outre, le procédé 50 d'authentification comporte une étape 56 d'émission, par l'unité centrale 22 et suite à la réception du signal de requête DC, d'un signal acoustique à destination du dispositif de commande 24.

Le signal acoustique comporte des données de vérification qui sont déterminées en fonction des données de vérification incluses dans le signal de requête DC. Par exemple, les données de vérification incluses dans le signal acoustique sont identiques à celles incluses dans le signal de requête DC, ou obtenues en appliquant une ou plusieurs fonctions prédéfinies auxdites données de vérification incluses dans le signal de requête DC.

Dans le cas notamment où le module Bluetooth 222 et le haut-parleur 224 de l'unité centrale 22 forment un module de téléphonie mains-libres Bluetooth, les données de vérification se présentent par exemple sous la forme d'une trame audionumérique.

Par « trame audionumérique », on entend le résultat de la numérisation d'un signal acoustique et de sa compression éventuelle au moyen d'un codeur de source, tel qu'un codeur MP3, AAC, etc. Le signal acoustique émis par l'unité centrale 22 correspond alors à la traduction analogique de ladite trame audionumérique.

Le procédé 50 d'authentification illustré par la figure 4 comporte en outre une étape de comparaison (non illustrée), par le dispositif de commande 24, des données de

vérification reçues dans le signal acoustique avec les données de vérification émises dans le signal de requête DC.

Au cours de l'étape de comparaison, le dispositif de commande 24 détermine si les données de vérification reçues ont été déterminées à partir des données de vérification émises.

Si les données de vérification reçues ont été déterminées à partir des données de vérification émises, le dispositif de commande 24 considèrera qu'il se trouve à l'intérieur du véhicule automobile 10. Dans le cas contraire, le dispositif de commande 24 considèrera qu'il se trouve à l'extérieur du véhicule automobile 10 et le démarrage du véhicule automobile devra être refusé.

Il est à noter que les données de vérification peuvent être des données d'authentification, ou tout type de données adaptées à permettre au dispositif de commande 24 de détecter le signal acoustique, et de déterminer si les données de vérification reçues ont bien été déterminées à partir des données de vérification émises.

Si les données de vérification reçues dans le signal acoustique ont bien été déterminées en fonction des données de vérification du signal de requête DC, le procédé 50 d'authentification comporte par exemple une étape 58 d'émission, par le dispositif de commande 24, d'un signal radioélectrique à destination de l'unité centrale 22, dit « signal de réponse », comportant des données d'authentification.

Le procédé 50 d'authentification comporte de préférence une étape 52 d'émission, par l'unité centrale 22, d'un signal radioélectrique à destination du dispositif de commande 24, dit « signal de requête UC ». Le signal de requête UC est émis avant le signal de réponse et les données d'authentification incluses dans le signal de réponse sont de préférence déterminées en fonction des données d'authentification incluses dans le signal de requête UC.

Tel qu'indiqué précédemment, le procédé 50 d'authentification illustré par la figure 4 est particulièrement adapté à une mise en œuvre par un système 20 d'authentification tel que décrit en référence à la figure 2. Rien n'exclut cependant de mettre en œuvre le procédé 50 d'authentification illustré par la figure 4 au moyen par exemple d'un système 20 d'authentification tel qu'illustré par la figure 1. En outre, rien n'exclut, suivant des modes particuliers de mise en œuvre, de combiner tout ou partie des étapes des procédés 50 d'authentification illustrés par les figures respectivement 3 et 4.

La description ci-avant illustre clairement que par ses différentes caractéristiques et leurs avantages, la présente invention atteint les objectifs qu'elle s'était fixés.

En particulier, l'émission d'un signal acoustique à l'intérieur du véhicule automobile 10 permet d'évaluer si le dispositif de commande 24 se trouve à l'intérieur

dudit véhicule automobile. Ainsi, la proximité du dispositif de commande 24 peut être vérifié grâce à l'émission / détection du signal acoustique, tandis que tout ou partie des données d'authentification sont échangées sous la forme de signaux radioélectriques, par l'intermédiaire de modules de communication sans fil GPRS, UMTS, WiFi, Bluetooth, etc., qui permettent d'avoir un débit de données plus important.

En vue d'une intégration du dispositif de commande 24 dans un téléphone portable, la détection du signal acoustique peut être effectuée au moyen d'un microphone du téléphone portable, de sorte que la détection du signal acoustique par le téléphone portable peut être rendue possible par une simple mise à jour logicielle dudit téléphone portable.

REVENDICATIONS

1 - Procédé (50) d'authentification d'un dispositif de commande (24) vis-à-vis d'une unité centrale (22) d'un véhicule (10), l'authentification dudit dispositif de commande s'effectuant au cours d'une session d'authentification en échangeant des données d'authentification entre ledit dispositif de commande et ladite unité centrale sous la forme de signaux radioélectriques, caractérisé en ce qu'il comporte l'évaluation de la présence du dispositif de commande (24) à l'intérieur du véhicule (10) par l'émission, à l'intérieur dudit véhicule, d'un signal acoustique par l'unité centrale (22), ledit dispositif de commande (24) ne pouvant être considéré comme étant à l'intérieur du véhicule (10) que lorsque ledit dispositif de commande (24) a détecté ledit signal acoustique.

2 - Procédé (50) selon la revendication 1, caractérisé en ce qu'une partie des données d'authentification formées par l'unité centrale (22) sont émises, de ladite unité centrale vers le dispositif de commande (24), par l'intermédiaire du signal acoustique.

3 - Procédé (50) selon la revendication 2, caractérisé en ce qu'il comporte les étapes suivantes :

- étape (52) d'émission, par l'unité centrale (22), d'un signal radioélectrique à destination du dispositif de commande (24), dit « signal de requête UC », comportant des données d'authentification,
- étape (58) d'émission, par le dispositif de commande (24) et suite à la réception du signal de requête UC et du signal acoustique, d'un signal radioélectrique à destination de l'unité centrale (22), dit « signal de réponse », comportant des données d'authentification déterminées en fonction des données d'authentification incluses dans le signal de requête UC et dans le signal acoustique.

4 - Procédé (50) selon la revendication 1, caractérisé en ce que :

- ledit procédé comporte une étape (54) d'émission, par le dispositif de commande (24), d'un signal radioélectrique à destination de l'unité centrale dit « signal de requête DC », comportant des données de vérification,
- le signal acoustique comporte des données de vérification déterminées en fonction des données de vérification incluses dans le signal de requête DC,
- ledit procédé comporte une étape de comparaison, par le dispositif de commande (24), des données de vérification reçues dans le signal acoustique avec les données de vérification émises dans le signal de requête DC.

5 - Procédé (50) selon la revendication 4, caractérisé en ce que les données de vérification incluses dans le signal de requête DC se présentent sous la forme d'une trame audionumérique, et en ce que le signal acoustique correspond à la traduction analogique de ladite trame audionumérique.

6 - Procédé (50) selon l'une des revendications 4 à 5, caractérisé en ce que, lorsque les données de vérification reçues dans le signal acoustique ont été déterminées en fonction des données de vérification du signal de requête DC, ledit procédé comporte une étape (52) d'émission, par le dispositif de commande (24), d'un signal radioélectrique à destination de l'unité centrale (22), dit « signal de réponse », comportant des données d'authentification déterminées en fonction de données d'authentification incluses dans un signal radioélectrique préalablement reçu de l'unité centrale (22).

7 - Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comporte une étape (56) d'émission, par l'unité centrale (22), d'un signal radioélectrique à destination du dispositif de commande (24), dit « signal de réveil », ledit signal de réveil étant émis avant d'émettre le signal acoustique.

8 - Système (20) d'authentification comportant un dispositif de commande (24) à authentifier vis-à-vis d'une unité centrale (22) d'un véhicule (10), ledit dispositif de commande et ladite unité centrale comportant chacun :

- un module d'authentification (240, 220) adapté à former des données d'authentification,
- un module de communication sans fil (242, 222) adapté à émettre et recevoir des signaux radioélectriques comportant des données d'authentification,

caractérisé en ce que le système (20) d'authentification est configuré pour évaluer la présence du dispositif de commande (24) à l'intérieur du véhicule (10) par l'émission, à l'intérieur dudit véhicule, d'un signal acoustique par un module d'émission acoustique (224) de l'unité centrale (22), ledit dispositif de commande (24) ne pouvant être considéré comme étant à l'intérieur du véhicule (10) que lorsque ledit signal acoustique a été détecté par ledit dispositif de commande (24) comportant un module de réception acoustique (244).

9 - Système (20) selon la revendication 8, caractérisé en ce que l'unité centrale (22) est adaptée à émettre des données d'authentification, formées par le module d'authentification (220) de ladite unité centrale, par l'intermédiaire du module d'émission acoustique (224), et/ou l'unité centrale (22) est adaptée à émettre un signal acoustique correspondant à une trame audionumérique reçue par l'intermédiaire du module de

communication sans fil (222) de ladite unité centrale, sans passer par le module d'authentification (220) de ladite unité centrale.

10 - Véhicule (10) caractérisé en ce qu'il comporte un système (20) d'authentification selon l'une des revendications 8 à 9.

Fig 1

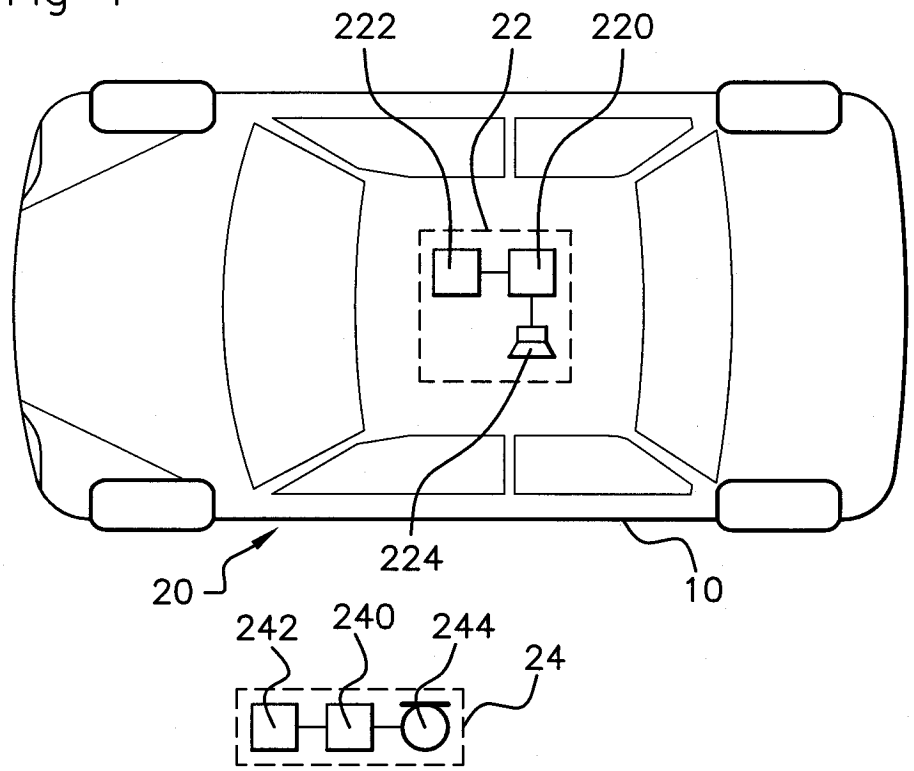

222
22
220
224
20
10
242
240
244
24

Fig 2

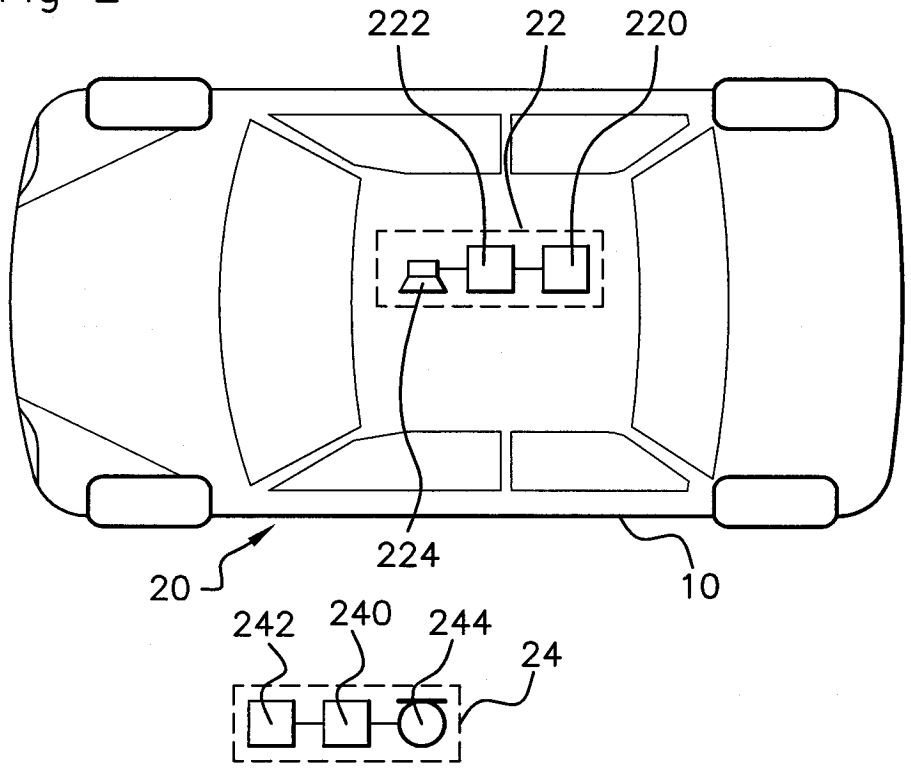

222
22
220
224
20
10
242
240
244
24

Fig 3

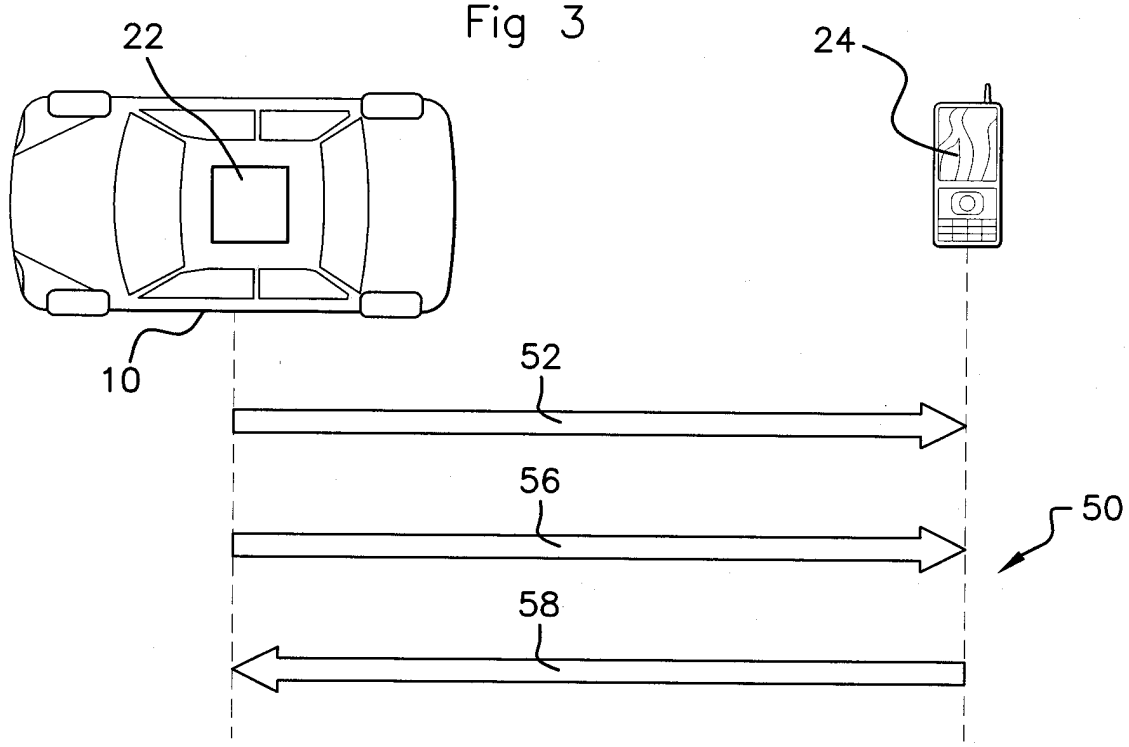
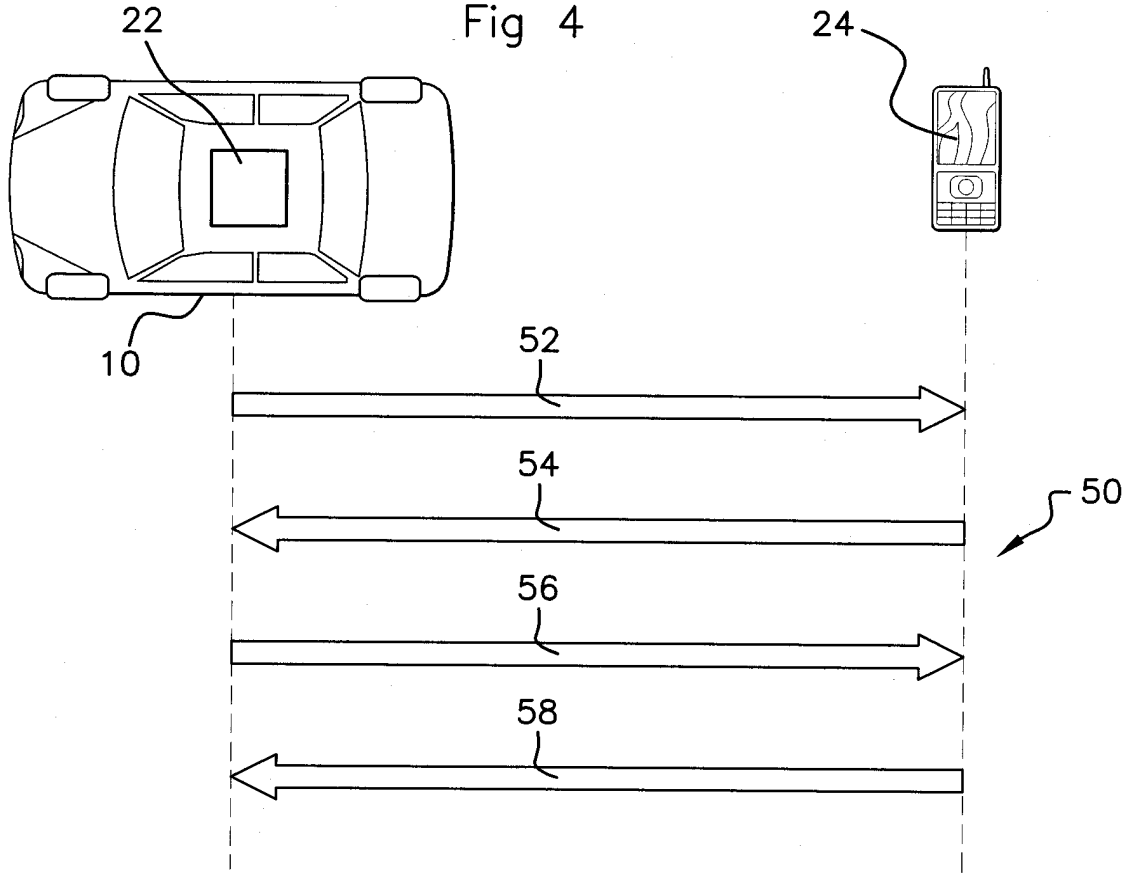


Fig 4



RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 763955
FR 1200308

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	DE 42 40 426 A1 (SCHMITZ THOMAS [DE]) 9 juin 1994 (1994-06-09) * colonne 2, ligne 57-67 * * colonne 4, ligne 11-19; revendication 7; figures 1,2 *	1,8-10	H04W12/06
X	US 5 831 520 A (STEPHAN CRAIG HAMMANN [US]) 3 novembre 1998 (1998-11-03) * colonne 3, ligne 59 - colonne 4, ligne 2 * * colonne 4, ligne 12-26 * * colonne 6, ligne 12-46; figure 1 *	1,8-10	
X	US 2008/258553 A1 (CHRISTENSON KEITH A [US] ET AL) 23 octobre 2008 (2008-10-23) * abrégé * * alinéas [0020], [0025]; figure 3 *	1,8-10	
A	KR 2007 0111139 A (HYUNDAI AUTONET CO LTD [KR]) 21 novembre 2007 (2007-11-21) * abrégé; figure 1 *	1-10	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
A	US 2011/210830 A1 (TALTY TIMOTHY J [US] ET AL) 1 septembre 2011 (2011-09-01) * abrégé; figures 4,6,8 *	2-7	B60R H04W
A	US 2010/227549 A1 (KOZLAY ALAN [US]) 9 septembre 2010 (2010-09-09) * abrégé * * alinéas [0007], [0017], [0022]; figures 1,3 *	2-7	
A	US 2008/268776 A1 (AMENDOLA RAFFAELE G [US]) 30 octobre 2008 (2008-10-30) * alinéas [0018], [0023]; figures 1-3 *	2-7	

Date d'achèvement de la recherche	Examinateur
26 octobre 2012	Sleightholme-Albanis

CATÉGORIE DES DOCUMENTS CITÉS

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 bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1200308 FA 763955

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 26-10-2012
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
DE 4240426 A1	09-06-1994	AUCUN	
US 5831520 A	03-11-1998	DE 69925651 D1	14-07-2005
		DE 69925651 T2	04-05-2006
		EP 0931896 A2	28-07-1999
		JP 11256902 A	21-09-1999
		US 5831520 A	03-11-1998
US 2008258553 A1	23-10-2008	CN 101295412 A	29-10-2008
		DE 102008015938 A1	30-10-2008
		US 2008258553 A1	23-10-2008
KR 20070111139 A	21-11-2007	AUCUN	
US 2011210830 A1	01-09-2011	CN 102170299 A	31-08-2011
		DE 102011011843 A1	29-03-2012
		US 2011210830 A1	01-09-2011
US 2010227549 A1	09-09-2010	AUCUN	
US 2008268776 A1	30-10-2008	AUCUN	

EPO FORM P0465