(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 908 205**

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

(21) **N° d'enregistrement national :** **06 09610**

(51) Int Cl[8] : **G 06 K 19/073** (2006.01), G 06 K 7/08, 9/00, H 04 L 9/32, G 06 F 21/00

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 03.11.06.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 09.05.08 Bulletin 08/19.

(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) :** *XIRING Société anonyme* — FR.

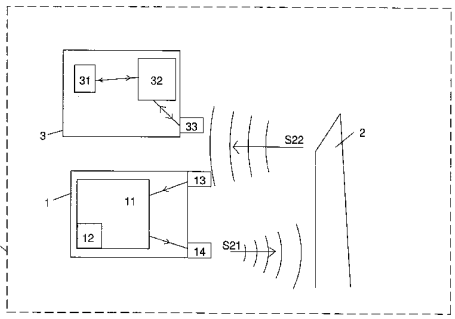
(72) **Inventeur(s) :** DEBORGIES LUC.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** CABINET DEBAY.

(54) DISPOSITIF DE PROTECTION CONTRE LA FRAUDE DES OBJETS DE COMMUNICATION SANS CONTACT.

(57) L'invention concerne un dispositif (1) simple de protection contre une intrusion accidentelle ou frauduleuse d'au moins un objet (3) de communication sans contact à circuit (31, 32) intelligent mémorisant des informations sensibles ou des informations donnant accès à des services, le circuit électronique de l'objet protégé restant inchangé, notamment grâce à des moyens (13) de réception de signaux (S22) radio dans une plage de fréquences de l'ordre du mégahertz à quelques dizaines de mégahertz, les signaux radio reçus générant l'énergie de fonctionnement pour activer un circuit (11) intelligent générateur d'un signal de brouillage à émettre par des moyens (14) d'émission du dispositif de protection sous la forme d'ondes (S21) radio de brouillage et des moyens (12) d'interruption validant ou invalidant le fonctionnement du dispositif de protection.



FR 2 908 205 - A1

Dispositif de protection contre la fraude des objets de communication sans contact

L'invention concerne le domaine des communications sans contact entre d'une part une borne ou un lecteur sans contact, et d'autre part des objets de communication sans contact. L'invention concerne notamment un dispositif de sécurisation des objets de communication sans contact.

Les objets de communication sans contact, comme par exemple les cartes à circuit intégré communicant sans contact, sont utilisés, de façon très variée, par exemple pour effectuer un paiement, réaliser une identification du porteur de l'objet de communication sans contact ou stocker des informations. Des cartes de ce type sont, par exemple, utilisées pour le contrôle d'accès ou le paiement automatique dans le métro. L'utilisateur passe simplement sa carte à proximité d'une borne, par exemple, contrôlant l'accès au métro, pour activer la carte qui communique à la borne les informations nécessaires pour certifier la validité d'un abonnement. L'utilisation d'une carte à circuit intégré communicant sans contact, avec un terminal ou une borne ou un lecteur sans contact, permet, par exemple, à l'utilisateur de gagner beaucoup de temps.

Dans ce type de système de communication entre une borne ou un lecteur sans contact et un objet de communication sans contact, la communication est réalisée par émission d'ondes de radiofréquence. La norme ISO/IEC 14443, établie par l'Organisme International de Normalisation et la Commission Internationale sur l'Electrotechnique, définit par exemple un ensemble de règles concernant les cartes d'identification, les cartes à circuit intégré sans contact et les cartes de proximité. Conformément à cette norme, la borne ou le lecteur sans contact émet des signaux de radiofréquence, dans un spectre de fréquences déterminé autour de 13,56MHz, pour transmettre des informations et de l'énergie d'alimentation à la carte sans contact. D'autres caractéristiques de cette norme concernent, par exemple,

des règles anti-collision lorsqu'une borne ou un lecteur sans contact communique avec plusieurs cartes simultanément.

Cependant les applications réalisées par des objets de communication sans contact ne sont généralement pas sécurisées. En effet les objets de communication sans contact, comme par exemple des cartes, s'activent, généralement, automatiquement lors de leur passage dans un domaine de portée d'une borne ou d'un lecteur sans contact, le domaine de portée correspondant à une région de l'espace autour de la borne ou du lecteur, dans laquelle le signal de radiofréquence émis par la borne ou le lecteur a une puissance suffisante pour activer l'objet de communication sans contact. Ainsi le porteur d'une carte de paiement par communication sans contact pourrait être taxé, sans raison valable, de façon accidentelle ou par une borne ou un lecteur pirate. Un problème technique des cartes ou des objets de communication sans contact est donc de protéger ces cartes ou ces objets contre d'éventuelles intrusions ou contre une utilisation involontaire.

De plus un objet de communication sans contact, comme par exemple une carte, peut généralement être utilisé par n'importe quel utilisateur. Une carte volée d'accès au métro permet, par exemple, d'ouvrir les portails d'accès payant. Un autre problème technique des cartes ou des objets de communication sans contact est donc de permettre leur utilisation par un utilisateur ou un groupe d'utilisateurs déterminé, afin par exemple de protéger ces cartes ou ces objets contre le vol.

La demande de brevet WO 2005/031663 enseigne un dispositif de paiement relatif aux cartes de paiement sans contact, sécurisé par la mesure d'un paramètre biométrique de l'utilisateur. Un lecteur du paramètre biométrique communique ainsi avec la carte de paiement pour autoriser l'activation de la carte et réaliser un paiement, la carte étant, par défaut, par exemple, dans un état non activé. Cependant la réalisation d'un tel dispositif de paiement sécurisé, nécessite de modifier l'agencement du circuit électronique de la carte de paiement sans contact pour avoir d'une part une liaison sécurisée de communication entre le lecteur biométrique et la carte de

paiement et d'autre part une liaison de communication avec une borne de paiement commandée dans un état activé ou désactivé. Ces modifications complexes apportées dans une carte de paiement dont le volume est très limité, sont donc très coûteuses. De plus un tel dispositif de sécurité nécessite d'avoir un lecteur biométrique associé à chaque carte de paiement.

La présente invention a pour objectif de pallier un ou plusieurs inconvénients de l'art antérieur en proposant un dispositif de protection pour objet de communication sans contact, l'objet de communication sans contact communicant avec une borne ou un lecteur sans contact, étant protégé de façon simple, contre une intrusion accidentelle ou frauduleuse, sans nécessiter de modification dans l'agencement du circuit électronique de cet objet.

Cet objectif est atteint grâce à un dispositif de protection pour objet de communication sans contact à circuit intelligent mémorisant des informations sensibles ou des informations donnant accès à des services, caractérisé en ce que le dispositif de protection comprend au moins des moyens de réception radio de premiers signaux radio émis par une borne ou un lecteur sans contact, dans une plage de fréquences de l'ordre du mégahertz à quelques dizaines de mégahertz, les premiers signaux reçus générant l'énergie de fonctionnement du dispositif de protection pour activer un circuit intelligent du dispositif de protection générateur d'un signal de brouillage à émettre par des moyens d'émission du dispositif de sécurisation sous la forme d'ondes radio de brouillage destinées à la borne ou au lecteur, les ondes radio de brouillage étant produites à la réception des premiers signaux avec une puissance suffisante pour être reçues par des moyens de réception radio de la borne ou du lecteur et détériorer la réception par les moyens de réception radio de la borne ou du lecteur de seconds signaux radio émis par l'objet de communication sans contact, en réponse à l'activation par la borne ou le lecteur, et des moyens d'interruption pour valider ou invalider le dispositif de protection.

Selon une autre particularité, l'objet de communication sans contact, protégé par le dispositif de protection, est activé dans un domaine de portée de la borne ou du lecteur, la borne ou le lecteur, émettant les premiers signaux radio par des moyens d'émission radio, pour communiquer avec l'objet de communication sans contact et alimenter l'objet de communication sans contact, en énergie par des moyens de réception radio de l'objet de communication sans contact,

l'objet de communication sans contact émettant les seconds signaux radio, par des moyens d'émission radio de l'objet de communication sans contact, pour communiquer avec la borne ou le lecteur, par les moyens de réception radio de la borne ou du lecteur.

Selon une autre particularité, les moyens de réception radio de l'objet de communication sans contact et les moyens de réception radio du dispositif de protection comprennent chacun une bobine appartenant à un circuit résonnant accordé déterminé.

Selon une autre particularité, les moyens d'émission radio de l'objet de communication sans contact et les moyens d'émission radio du dispositif de protection comprennent chacun la bobine dans le circuit résonnant accordé utilisé pour la réception radio.

Selon une autre particularité, la communication, entre d'une part la borne ou le lecteur et d'autre part l'objet de communication sans contact, étant réalisée selon un protocole anti-collision déterminé, l'objet de communication sans contact émettant les seconds signaux radio en réponse aux premiers signaux radio après au moins après l'émission d'une requête par les premiers signaux, le circuit intelligent du dispositif de protection commande une émission des ondes radio de brouillage en réponse aux premiers signaux radio, l'émission des ondes radio de brouillage se maintenant durant la réception des premiers signaux.

Selon une autre particularité, le signal de brouillage, reçu par la borne ou le lecteur, est représentatif de données déterminées traitées par des moyens de traitement de la borne ou du lecteur, pour provoquer une réinitialisation dans l'exécution du protocole anti-collision.

Selon une autre particularité, le signal de brouillage, reçu par la borne ou le lecteur, est représentatif de données déterminées traitées par des moyens de traitement de la borne ou du lecteur pour provoquer une saturation des moyens de traitement.

Selon une autre particularité, le signal de brouillage généré, lors de la réception des premiers signaux émis par la borne ou le lecteur, par le circuit intelligent du dispositif de protection, est un signal prédéterminé pour économiser l'énergie dépensée par le circuit intelligent en faveur de l'énergie utilisée par les moyens d'émission radio du dispositif de protection.

Selon une autre particularité, le circuit intelligent du dispositif de protection comprend un compteur diviseur de la fréquence de modulation des premiers signaux émis par la borne ou le lecteur.

Un autre objectif de la présente invention est de proposer un dispositif de protection contre le vol, en protégeant l'utilisation d'un objet de communication sans contact par des moyens d'identification.

Selon cet objectif, des moyens interactifs du dispositif de protection comprennent un capteur biométrique transmettant à un circuit d'authentification du dispositif de protection, commandant les moyens d'interruption, une information représentative d'un paramètre biométrique mesuré, comparée avec au moins une information représentative d'un paramètre biométrique d'un utilisateur autorisé à utiliser l'objet de communication sans contact.

Selon une variante, des moyens interactifs du dispositif de protection comprennent un clavier alphanumérique transmettant à un circuit d'authentification du dispositif de protection, commandant les moyens d'interruption, une information représentative d'un code entré par un utilisateur, comparé avec au moins un code d'autorisation de l'utilisation de l'objet de communication sans contact.

Selon une autre particularité, les moyens d'interruption comprennent un interrupteur ou un bouton poussoir disposé à la surface du dispositif de protection ou dans un logement en creux aménagé dans l'épaisseur du dispositif de protection.

Selon une autre particularité, les moyens d'interruption comprennent un interrupteur ou un bouton poussoir disposé à l'extrémité d'une ligne de communication avec le dispositif de protection.

Un autre objectif de la présente invention est de pallier un ou plusieurs inconvénients de l'art antérieur en proposant un système portable de communication sans contact, dans lequel un objet de communication sans contact est protégé, de façon simple, contre une intrusion accidentelle ou frauduleuse, sans nécessiter de modification dans l'agencement du circuit électronique de l'objet.

Cet objectif est atteint grâce à un système sécurisé portable de communication sans contact comprenant au moins un objet de communication sans contact à circuit intelligent mémorisant des informations sensibles ou des informations donnant accès à des services, l'objet de communication sans contact comprenant des moyens de réception radio de signaux de communication et d'alimentation et des moyens d'émission radio de signaux de communication, une première bobine déterminée dans un premier circuit résonnant accordé appartenant aux moyens d'émission et de réception radio de l'objet de communication sans contact, le système étant caractérisé en ce qu'il comporte au moins :

un dispositif de protection comprenant des moyens de réception radio de signaux de communication et d'alimentation, dans une plage de fréquences de l'ordre du mégahertz à quelques dizaines de mégahertz, pour activer un circuit intelligent du dispositif de protection générateur d'un signal de brouillage à émettre par des moyens d'émission du dispositif de protection sous la forme d'ondes radio de brouillage, une seconde bobine déterminée dans un second circuit résonnant accordé appartenant aux moyens d'émission et de réception radio du dispositif de protection, le dispositif de protection comprenant des moyens d'interruption permettant de valider ou d'invalider le fonctionnement du dispositif de protection,

les moyens d'interruption du circuit de brouillage étant commandés, selon le résultat d'une comparaison effectuée, par des moyens de

comparaison entre d'une part une information provenant de moyens interactifs d'authentification et d'autre part une information mémorisée dans des moyens de mémorisation.

Selon une autre particularité, le dispositif de protection et l'objet de communication sans contact, sont rendus solidaires dans un boîtier à fermeture sécurisée, dont la fermeture valide le fonctionnement du dispositif de protection.

Selon une autre particularité, le boîtier sécurisé est moulé d'un seul bloc autour du dispositif de protection et de l'objet de communication sans contact.

Selon une autre particularité, le boîtier sécurisé est fermé autour du dispositif de protection et de l'objet de communication sans contact, l'ouverture du boîtier étant commandée par une clé sécurisée.

Un autre objectif de la présente invention est de permettre la protection d'une pluralité d'objets de communication sans contact par un même dispositif de protection.

Selon cet objectif, le boîtier sécurisé comporte un logement pour accueillir au moins un objet supplémentaire de communication sans contact mémorisant des informations sensibles ou des informations donnant accès à des services.

Un autre objectif de la présente invention est de proposer un système de communication sans contact protégé contre le vol, en protégeant son utilisation par des moyens d'identification.

Selon cet objectif, les moyens interactifs d'authentification comprennent un clavier alphanumérique transmettant aux moyens de comparaison, une information représentative d'un code entré par un utilisateur, comparé avec au moins un code d'autorisation de l'utilisation de l'objet de communication sans contact.

Selon une autre particularité, les moyens interactifs d'authentification comprennent un capteur biométrique transmettant aux moyens de comparaison, une information représentative d'un paramètre biométrique mesuré, comparée avec au moins une information représentative d'un

paramètre biométrique d'un utilisateur autorisé à utiliser l'objet de communication sans contact.

Selon une autre particularité, le capteur biométrique est un capteur d'empreinte digitale.

Selon une autre particularité, le capteur d'empreinte digitale est un lecteur optique devant lequel l'utilisateur passe son doigt.

Selon une autre particularité, le capteur biométrique est un lecteur d'iris.

Selon une autre particularité, le capteur biométrique est un analyseur d'empreinte vocale.

Selon une autre particularité, les moyens interactifs d'authentification et les moyens de comparaison comprennent des moyens d'alimentation pour réaliser la comparaison et commander les moyens d'interruption avant l'entrée du système sécurisé dans le domaine de portée.

Un autre objectif de la présente invention est de pallier un ou plusieurs inconvénients de l'art antérieur en proposant un dispositif simple de protection d'un objet de communication sans contact, contre une intrusion accidentelle ou frauduleuse, sans nécessiter de modification dans l'agencement du circuit électronique de l'objet et conçu pour s'adapter aux appareils existants.

Cet objectif est atteint par un dispositif de protection d'au moins un objet de communication sans contact à circuit intelligent mémorisant des informations sensibles ou des informations donnant accès à des services, caractérisé en ce qu'il comprend au moins des moyens de réception de signaux radio dans une plage de fréquences de l'ordre du mégahertz à quelques dizaines de mégahertz, les signaux radio reçus générant l'énergie de fonctionnement du dispositif de protection pour activer un circuit intelligent générateur d'un signal de brouillage à émettre par des moyens d'émission du dispositif de protection sous la forme d'ondes radio de brouillage, une bobine déterminée dans un circuit résonnant accordé appartenant aux moyens d'émission et de réception radio du dispositif de protection, et des moyens

d'interruption validant ou invalidant le fonctionnement du dispositif de protection.

Selon une autre particularité, le signal de brouillage est émis dès réception des premiers signaux avant la fin d'une requête conforme à un protocole de communication.

Selon une autre particularité, au moins les moyens d'émission et de réception radio du dispositif de protection et le circuit intelligent du dispositif de protection sont insérés dans un boîtier de mêmes dimensions que l'objet de communication sans contact à circuit intelligent protégé.

Selon une autre particularité, les moyens d'interruption comprennent un interrupteur disposé à la surface du dispositif de protection ou dans un logement en creux aménagé dans l'épaisseur du dispositif de protection.

Selon une autre particularité, les moyens d'interruption comprennent un interrupteur disposé à l'extrémité d'une ligne de communication avec le dispositif de protection.

L'invention, ses caractéristiques et ses avantages apparaîtront plus clairement à la lecture de la description faite en référence aux figures référencées ci-dessous :

- la figure 1 représente un exemple de système de communication sans contact sécurisé selon l'invention ;

- la figure 2 représente un schéma électronique d'un exemple de dispositif de protection selon l'invention ;

- la figure 3 représente une vue en perspective d'un exemple de dispositif de protection selon l'invention, au format d'une carte de crédit et équipé d'un interrupteur ;

- la figure 4 représente une vue en perspective d'un exemple de dispositif de protection selon l'invention, équipé d'une télécommande ;

- la figure 5 représente une vue en perspective d'un ensemble de communication sans contact selon l'invention sécurisé par un clavier pour entrer un code secret ;

- les figures 6, 7 et 8 représentent chacune une vue en perspective d'un ensemble de communication sans contact selon l'invention sécurisé par un lecteur d'un paramètre biométrique.

L'invention va à présent être décrite en référence aux figures précédemment citées. Un dispositif (1) de protection est utilisé avec un ou plusieurs objets (3), par exemple portatifs, établissant une communication sans contact avec une borne (2) ou un lecteur. Les objets de communication sans contact (3) sécurisés sont disposés dans un domaine (20) de portée de la borne ou le lecteur, pour être alimentés par les ondes (S22) radio, émises par la borne (2) ou le lecteur, et établir une communication sans contact avec celle-ci. Le dispositif (1) de protection est placé dans le domaine (20) de portée, en même temps qu'un ou plusieurs objets (3) de communication sans contact à protéger. Dans le domaine de portée le champ électromagnétique a par exemple, de manière non limitative, une valeur comprise entre 1A/m et 10A/m.

Comme représenté à la figure 1, le dispositif (1) de sécurisation est disposé dans le domaine (20) de portée de la borne (2) de communication ou du lecteur, pour sécuriser l'objet (3) de communication sans contact à circuit intelligent mémorisant des informations sensibles ou des informations donnant accès à des services. Le dispositif (1) de protection se trouve donc dans le domaine (20) de la borne ou du lecteur, de même que le ou les objets de communication protégés par le dispositif de protection. L'objet (3) de communication sans contact comprend par exemple un espace (31) mémoire comprenant les informations sensibles ou donnant accès à des services, en communication avec un circuit (32) d'alimentation et de traitement. Le circuit (32) d'alimentation et de traitement est relié, d'autre part, à des moyens de communication et d'alimentation par des ondes radio, comprenant par exemple une antenne (33).

Le dispositif (1) de sécurisation comprend des moyens (13) de réception et d'alimentation radio en communication avec des moyens d'alimentation et des moyens de traitement, par exemple sous la forme d'un circuit (11) d'alimentation et de traitement, activé ou désactivé par des

moyens (12) d'interruption. Les moyens (12) d'interruption comprennent par exemple un interrupteur (101) ou un bouton poussoir, pour autoriser ou non le fonctionnement du dispositif (1) de sécurisation. L'interrupteur (101) est, de manière non limitative, un interrupteur à contact actionné mécaniquement ou un interrupteur électronique comprenant, par exemple, un transistor commandé. L'interrupteur est par exemple positionné par un bouton poussoir réalisant ou non un contact électrique selon sa position.

Selon un autre exemple de réalisation, un interrupteur à transistor, comme par exemple un transistor de puissance, est commandé par des moyens de commande électroniques, dans une position passante ou bloquée, selon un paramètre d'entrée. Le paramètre d'entrée est par exemple la position d'un bouton de commande ou le résultat d'une comparaison entre une information numérique mémorisée et une information représentative d'un paramètre biométrique produit par un capteur. De manière non limitative, la comparaison est effectuée dans un dispositif d'authentification ou dans le dispositif (1) de sécurisation. Selon un autre exemple de réalisation, sans sortir de l'esprit de l'invention, la comparaison est effectuée dans l'objet de communication protégé.

Lorsque les moyens (12) d'interruption sont placés dans une position d'autorisation de fonctionnement, un signal (S22) radiofréquence reçu par les moyens (13) de réception, déclenche l'alimentation du dispositif (1) de protection, par ses moyens d'alimentation. Le circuit (11) d'alimentation et de traitement, par exemple, alimenté en énergie, comprend des moyens de traiter le signal radiofréquence reçu pour émettre un signal (S21) radiofréquence de brouillage par des moyens (14) d'émission du dispositif (1) de protection.

Lorsque les moyens (12) d'interruption sont placés dans une position d'interdiction du fonctionnement, le dispositif (1) de protection n'émet plus de signal radio de brouillage. Les moyens d'interruption comprennent par exemple un interrupteur (101) pour commander, de manière non limitative, l'activation ou la désactivation des moyens de réception, des moyens d'alimentation, des moyens de traitement ou des moyens d'émission.

Un signal (S22) radiofréquence, émis par une borne (2) ou un lecteur sans contact, couvre son domaine (20) de portée et diffuse de l'énergie en même temps qu'une information. Ce signal (S22) est par exemple utilisé par l'objet (3) de communication sans contact à circuit intelligent, en partie pour son alimentation en énergie et en partie pour recevoir et traiter l'information contenue. Le signal (S22) émis par la borne (2) ou le lecteur est par exemple émis avec une première fréquence de modulation déterminée selon un premier type de modulation déterminée. Le signal émis par l'objet (3) de communication sans contact à circuit intelligent, est par exemple émis avec une deuxième fréquence de modulation déterminée selon un deuxième type de modulation déterminée. Pour brouiller cette communication, lors de son activation, le dispositif (1) de sécurisation comprend des moyens d'alimentation, des moyens de réception et de démodulation et des moyens d'émission et de modulation compatible avec la borne ou le lecteur, par exemple, de manière non limitative, identiques à ceux de l'objet (3) de communication sans contact à circuit intelligent. De manière non limitative, lors de la réception d'un signal, (S22) émis par la borne ou le lecteur, le signal (S21) de brouillage est représentatif d'informations dépendantes ou non des informations reçues. De manière non limitative, le signal (S21) de brouillage est représentatif d'un message aléatoire, d'une suite de « 1 », d'une suite de « 0 » ou d'un message résultant du traitement du message reçu.

De manière non limitative, un type d'objet de communication sans contact, sécurisé par le dispositif de protection, est, par exemple, décrit dans la demande de brevet WO 98/26370. Les objets communiquant sans contact sont, de manière non limitative, des objets portables réalisés au format standard des cartes de crédit. Le dialogue entre la borne de communication ou le lecteur sans contact, et les objets de communication sans contact est, par exemple, décrit dans le brevet EP 0 472 472.

Le dispositif (1) de sécurité est aussi utilisé, de manière non limitative, pour sécuriser un ou plusieurs objets (3) de communication sans contact, comme les cartes d'identification, les cartes à circuit intégré sans

contact ou les cartes de proximité conformes à la norme ISO/IEC 14443, définie par l'Organisme International de Normalisation et la Commission Internationale sur l'Electrotechnique. L'édition 2001 de la norme ISO/IEC 14443 sur les cartes d'identification, les cartes à circuit intégré sans contact ou les cartes de proximité, est subdivisée en quatre parties. Une première partie désignée par ISO/IEC14443-1:2001, porte sur les caractéristiques physiques de ces cartes. Une seconde partie désignée par ISO/IEC14443-2:2001, porte sur l'interface radio fréquence et les signaux de communication et notamment sur les éléments à fournir pour l'alimentation de la carte et la communication bidirectionnelle entre la carte et la borne ou le lecteur. Une troisième partie désignée par ISO/IEC14443-3:2001, porte sur l'initialisation et l'anti-collision et notamment sur les méthodes pour communiquer avec une carte dans un environnement comprenant plusieurs cartes. Une quatrième partie désignée par ISO/IEC14443-4:2001, porte sur le protocole de transmission.

Le signal (S21) de brouillage est émis à la réception du signal (S22) émis par la borne (2) ou le lecteur, lorsque les moyens d'interruption du dispositif de protection, sont dans une position d'autorisation du fonctionnement. L'émission, commandée par les moyens de traitement du dispositif de protection, est réalisée, de manière non limitative, dès la réception du signal ou après une temporisation déterminée. Le signal (S21) de brouillage est ainsi répété pour chaque signal (S22) reçu, émis par la borne (2) ou le lecteur. Tandis qu'un objet (3) de communication sans contact à circuit intelligent respecte des créneaux temporels d'autorisation d'émission ou d'attente d'émission, le dispositif de sécurisation émet un signal de brouillage tant que ses moyens d'alimentation fournissent de l'énergie. Une borne (2) ou un lecteur sans contact, fonctionnant par exemple selon la norme ISO/IEC 14443 établit par exemple un dialogue avec un ou plusieurs objets (3) de communication sans contact à circuit intelligent selon un protocole déterminé de communication dans des créneaux temporels, également appelés slots. Le signal (S21) de brouillage est émis par le dispositif de brouillage en même temps que le signal (S22) émis par la borne

ou le lecteur, en même temps qu'un signal émis par un objet (3) de communication sans contact à circuit intelligent ou dans un créneau temporel normalement inoccupé. Un créneau temporel normalement inoccupé est par exemple, un temps d'attente d'émission par l'objet (3) de communication sans contact, après la réception d'un signal (S22) émis par la borne (2) ou le lecteur. Ainsi le message représentatif d'un signal émis par un objet (3) de communication sans contact est brouillé par le signal (S21) additionnel de brouillage. De plus le protocole de communication, utilisé par la borne (2) ou le lecteur, devient complètement inutilisable. Ce type de protocole, qui commence par exemple par une étape d'initialisation, reste bloqué, de manière non limitative, à l'étape d'initialisation.

De façon avantageuse, le dispositif de sécurisation selon l'invention, est ajouté à un système de communication fonctionnel entre une borne ou un lecteur sans contact, et un ou plusieurs objets (3) de communication sans contact à circuit intelligent, pour réaliser un mur virtuel entre la borne (2) ou le lecteur, et le ou les objets (3) de communication sans contact, sans modification de la structure du système de communication existant. Un utilisateur empêche ainsi, en activant le dispositif de sécurité, une intrusion dans les informations sensibles ou les informations donnant accès à des services, contenues dans son objet (3) de communication sans contact à circuit intelligent. Pour utiliser son objet (3) de communication sans contact, l'utilisateur désactive le dispositif de sécurité par les moyens de commutation.

De façon avantageuse, le dispositif (2) de sécurité selon l'invention, alimenté par radio fréquences, utilise les mêmes sources d'énergie pour son alimentation, que l'objet (3) de communication sans contact protégé. De manière non limitative les moyens de réception comprennent une antenne utilisée aussi par les moyens d'émission pour émettre le signal de brouillage. La fréquence porteuse du signal reçu ou émis par le dispositif de sécurité est par exemple une fréquence déterminée de type ondes courtes, comprise entre 1Mhz et 30Mhz.

De façon avantageuse le dispositif (1) de protection, comme représenté aux figures 3 et 4 est réalisé avec les dimensions d'une carte de crédit. Ainsi le dispositif (1) de protection est disposé, avec une carte de communication sans contact, dans un portefeuille, le dispositif (1) de protection étant activé ou désactivé. De cette façon lorsque la carte de communication sans contact est placée dans un domaine (20) de portée d'une borne (2) ou d'un lecteur sans contact, le dispositif (1) de protection est placé en même temps dans ce domaine (20) de portée pour sécuriser la carte lorsque le dispositif de protection est activé. Comme représenté à la figure 3 un bouton poussoir (1001), disposé sur le dispositif (1) de protection, commande mécaniquement ou électroniquement la position de l'interrupteur (101) pour activer ou désactiver le dispositif (1) de protection. Le bouton poussoir disposé dans un logement en creux dans le dispositif de protection, permet d'avoir une épaisseur minimum pour placer le dispositif de protection dans un portefeuille. Lorsque le dispositif de protection est activé et placé dans un portefeuille avec une carte de communication sans contact, l'utilisateur peut transporter son portefeuille en toute sécurité, sans risque d'intrusion par une borne radiofréquence ou un lecteur sans contact. Pour utiliser sa carte de communication sans contact, par exemple pour effectuer des paiements dans un espace commercial sécurisé, l'utilisateur désactive le dispositif de protection en basculant le bouton (1001) poussoir, le dispositif de protection restant par exemple sans son portefeuille.

La figure 4 représente une variante d'un dispositif (1) de protection désactivé par une télécommande (1004, 1003, 1002). Le dispositif (1) de protection est par exemple relié par un connecteur (1004) à un câble (1003) de communication bifilaire à l'extrémité duquel est relié un bouton (1002) poussoir positionné par l'utilisateur. Le bouton (1002) réalise directement une connexion électrique ou active ou désactive un circuit électronique de commande de l'interrupteur (101), relié au connecteur (1004). Le dispositif (1) de protection est par exemple disposé dans le portefeuille de l'utilisateur avec une carte de communication sans contact à sécuriser, le portefeuille étant dans la poche intérieure de la veste de l'utilisateur. Le câble part par

exemple du connecteur (1004), puis passe à l'intérieur de la manche de la veste jusqu'à la main de l'utilisateur qui peut d'une pression de la main, changer l'état du bouton poussoir (1002) pour produire, par le connecteur (1004), un signal de commande de désactivation du dispositif de protection. L'utilisateur commande ainsi des plages temporelles durant lesquelles la communication radiofréquence avec sa carte de communication sans contact est autorisée. Lorsque l'interrupteur (101) n'est pas activé, le dispositif de protection est par exemple activé, par défaut.

Selon un autre exemple de réalisation, l'objet portable de communication sans contact et le dispositif de protection sont réalisés sous la forme de solide compact, par exemple accroché à un même anneau porte-clefs.

Selon un exemple non limitatif de réalisation, comme représenté à la figure 2, le dispositif (1) de sécurité comprend un circuit (100) électronique activé dans le domaine (20) de portée d'une borne (2) ou d'un lecteur sans contact, lorsque son interrupteur (101) est dans une position d'activation, autorisant le fonctionnement du dispositif de sécurité.

De manière non limitative, l'interrupteur coupe le circuit (108) de réception pour empêcher ou autoriser, en même temps la réception de l'information et la réception de l'énergie d'alimentation.

Selon un autre exemple de réalisation, l'interrupteur (101) est connecté à une entrée d'un circuit (114) intelligent, l'état logique de cette entrée déterminant l'état du circuit intelligent (114) pour commander ou non l'émission d'onde de brouillage.

Selon un autre exemple de réalisation, l'interrupteur (101) coupe ou non le circuit d'émission (1220, 122) du reste du circuit pour empêcher l'émission d'ondes radio de brouillage.

Ce circuit (100) électronique comprend, de manière non limitative, une bobine (102), appartenant à un circuit résonnant accordé (108) rayonnant le champ en espace libre, pour capter un champ magnétique (S22) modulé en provenance de la borne (2) ou du lecteur, ou pour produire en réponse un signal de brouillage modulé (S21) de ce champ magnétique.

Les signaux sont, par exemple, modulés selon une fréquence porteuse d'environ 13MHz, pour une bobine, de manière non limitative, de l'ordre de 4 à une dizaine de spires. De manière non limitative, de façon avantageuse, le nombre de spires du dispositif (1) de protection étant supérieur au nombre de spires de l'objet (3) de communication protégé, le dispositif (1) de protection aura un temps minimum de réponse inférieur à celui de l'objet protégé, lors de la réception des signaux radio émis par la borne ou le lecteur. Le circuit (100) électronique du dispositif de sécurité comprend aussi des moyens convertisseurs (110, 112, 116), coopérant avec la bobine (102), pour transformer le champ (S22) magnétique capté par cette dernière en une tension continue (d) d'alimentation du circuit (100) électronique du dispositif (1) de sécurisation, ces moyens comprenant un étage de redressement (110) et un étage de filtrage (112). Un étage (116) régulateur est par exemple ajouté en série pour délivrer une tension (d) de valeur déterminée.

Le circuit (100) électronique du dispositif (1) de sécurité comprend, d'autre part, des moyens (108, 1220, 122) d'émission et des moyens (108, 110, 112, 120) de réception de données, coopérant également avec la bobine. Un étage (120) extracteur d'horloge, recevant en entrée le signal (a) recueilli aux bornes du circuit accordé (108), délivre en sortie un signal (c) appliqué à l'entrée d'horloge (C114) du circuit numérique (114) intelligent. L'étage (116) régulateur, stabilisateur de tension, délivre par exemple, en sortie, une tension continue, redressée, filtrée et stabilisée (d), appliquée notamment à une borne d'alimentation positive (V114) du circuit numérique (114) intelligent, dont l'autre borne (G114) d'alimentation est la masse. Un étage modulateur (122, 1220) opère, par exemple, par modulation de charge, cette technique consistant à faire varier de manière contrôlée le courant consommé par le circuit accordé (108) situé dans le champ magnétique environnant engendré par la borne ou le lecteur. Le circuit modulateur (122) comporte un élément résistif 124 (résistance rapportée ou, en technologie monolithique, composant de type MOS sans grille faisant office de résistance) en série avec un élément de commutation (126) (transistor MOS)

commandé par un signal (f) de modulation généré par une sortie (S114) du circuit numérique 114.

Les moyens de réception comportent, de manière non limitative, des moyens (118) démodulateurs du signal capté par la bobine (102), ces moyens démodulateurs (118) opérant sur le signal (b) délivré en sortie des étages de redressement (110) et de filtrage (112). Un circuit (118) démodulateur fournit par exemple un signal (e) représentatif des informations comprises dans le signal (S22) radio émis par la borne (2) ou le lecteur. Le signal (e) en sortie du circuit (118) de démodulation, est transmis à une entrée (E114) du circuit (114) pour être traité. Le circuit (114) exécute par exemple un programme de traitement résidant dans sa mémoire (M114) pour produire un signal (f) de brouillage. De manière non limitative, les moyens démodulateurs réalisent une modulation d'amplitude ou respectivement de phase, les moyens d'émission comportant des moyens modulateurs réalisant une modulation d'amplitude ou respectivement de phase. Dans une variante de réalisation, le signal en entrée du démodulateur provient directement du circuit (108) résonnant sans être redressé ou filtré.

Selon un autre exemple de réalisation, le circuit (100) électronique du dispositif (1) de protection ne comprend pas de moyens de démodulation pour extraire l'information dans le signal (S22) radio émis par la borne (2) ou le lecteur. Le circuit (120) extracteur d'horloge fournit par exemple le signal d'horloge en entrée (C114) d'un circuit (114) intelligent compteur diviseur par un entier, égal par exemple à 16. Le circuit intelligent (114) diviseur produit par exemple un signal (f) de brouillage transmis à un circuit (122, 1220) modulateur. Selon une variante de réalisation, le signal de brouillage modulé est représentatif d'un message résident en mémoire (M114), l'émission étant cadencée par le signal (c) d'horloge.

De manière non limitative, l'étage modulateur (122), est placé en aval des circuits de redressement (110) et de filtrage (112), ou en amont de ces circuits, comme illustré (1220) sur la figure 2, c'est-à-dire directement aux bornes du circuit résonnant (108).

De manière non limitative, le signal radio (S21) de brouillage est émis, par une commande du circuit (114) intelligent, dès que le circuit (100) électronique est alimenté ou après une temporisation déterminée ou après la détection, par le circuit (114) intelligent, de la fin d'émission.

De façon avantageuse, la simplicité des opérations logiques réalisées par le composant (114) intelligent, par exemple de type diviseur, nécessite peu de ressources énergétiques pour le fonctionnement du composant (114) intelligent, et permet d'avoir une puissance d'émission maximum.

Selon une variante de réalisation, comme représenté aux figures 5 à 8, le dispositif (1) de protection est scellé à l'objet (3) portatif de communication sans contact à sécuriser. Le scellement est par exemple réalisé avec des éléments rigides imbriqués dans l'objet (3) portatif de communication sans contact à sécuriser de façon à détruire ou rendre inutilisable cet objet (3) portatif en cas de séparation.

Selon un autre exemple, l'objet (3) portatif de communication sans contact à sécuriser et le dispositif (1) de sécurisation sont moulés dans une même pièce plastique.

Selon un autre exemple de réalisation, le dispositif de protection équipé d'un dispositif d'authentification, comprend en logement pour un ou plusieurs objets communicant sans contact, le logement étant ensuite fermé par des moyens de fermeture sécurisés. L'ouverture du logement, pour retirer les objets de communication sans contact, est par exemple réalisée grâce à une clé de sécurité. Les moyens de fermeture sécurisés comprennent par exemple des moyens de destruction des objets de communication sans contact. Les moyens de fermeture sécurisés comprennent par exemple des moyens d'écrasement d'une partie de l'objet de communication sans contact, pour invalider l'objet placé dans le logement, en cas d'effraction.

Dans les exemples de réalisation représentés aux figures 5 à 8, les moyens d'interruption activent ou désactivent le dispositif (1) de sécurisation par un dispositif (1010 ; 1011 ; 1012, 1013, 1014 ; 1015, 1016, 1017) d'authentification. De manière non limitative, le dispositif d'authentification

comprend des moyens d'alimentation ou est alimenté par les moyens d'alimentation du dispositif de sécurisation. Dans le cas où le dispositif d'authentification nécessite une puissance importante et comprend ses propres moyens (1020) d'alimentation, comme par exemple une pile ou une batterie d'alimentation, le dispositif d'authentification maintient les moyens d'interruption en position d'activation du dispositif de protection, lorsque ses moyens (1020) d'alimentation ne sont plus fonctionnels. Dans le cas par exemple où un dispositif d'authentification comprend une pile d'alimentation et que cette pile ne stocke plus d'énergie, l'interrupteur reste, par exemple, en position fermée pour permettre le fonctionnement du dispositif de sécurisation et empêcher une utilisation frauduleuses de l'objet (3) portable de communication sans contact à protéger. L'ensemble formé par l'objet (3) portable de communication sans contact et le dispositif (1) de protection équipé d'un dispositif d'authentification, est ainsi protégé contre les intrusions accidentelles ou frauduleuse et son utilisation est limitée à une personne ayant un accès valide auprès du dispositif d'authentification. Le dispositif d'authentification est par exemple configuré pour permettre l'utilisation par une seule personne ou par un groupe de personnes déterminées.

Selon un exemple de réalisation, le dispositif d'authentification comprenant des moyens (1020) d'alimentation, comprend des moyens de désactivation le dispositif (1) de protection quelque soit la position du dispositif de protection, par exemple hors d'un domaine (20) de portée d'une borne ou d'un lecteur sans contact. De manière non limitative, la commande de désactivation est réalisée pendant une durée de désactivation déterminée ou jusqu'à ce que le dispositif (1) de protection sorte du domaine (20) de portée. Le dispositif d'authentification, en communication avec le dispositif (1) de protection, comprend, par exemple, des moyens de détecter que le dispositif (1) de protection n'est plus alimenté, pour commander les moyens (101) d'interruption du dispositif (1) de protection dans une position autorisant le fonctionnement du dispositif (1) de protection.

Selon l'exemple de la figure 5, le dispositif (1) de protection est par exemple désactivé par un dispositif (1010) d'authentification comportant un

clavier. Lorsqu'un utilisateur tape le bon code d'identification sur le clavier, des premiers moyens de communication transmettent le code à des moyens de traitement du dispositif d'authentification, qui commandent, par des seconds moyens de communication, la désactivation du dispositif (1) de protection. Les moyens de traitement du dispositif d'authentification commandent par exemple l'interrupteur (101) dans une position ouverte ou fermée.

Selon une variante de réalisation, comme représenté à la figure 6, le dispositif (1) de protection est désactivé par un dispositif (1011) d'authentification par reconnaissance d'empreinte digitale. Des exemples non limitatifs de capteurs d'empreinte digitale sont : un capteur optique d'empreinte, un capteur électrique thermique, un capteur capacitif, un capteur de champ électrique ou un capteur de pression. Selon un exemple non limitatif de réalisation, un capteur d'empreinte digitale Authentec AES1510 ou un capteur d'empreinte digitale UPEK TCS3C ou un capteur d'empreinte digitale Veridicom est utilisé pour désactiver le dispositif de protection.

De manière non limitative, un capteur optique d'empreinte digitale réalise une capture d'une image représentative de l'empreinte ou réalise une capture d'une série d'images par un déplacement relatif de la partie du doigt comprenant l'empreinte digitale par rapport au lecteur optique d'empreinte. Le déplacement relatif du doigt par rapport au capteur optique, permet par exemple de réaliser une opération de type scannage. L'utilisateur déplace, par exemple, son doigt devant une barrette de lecture optique.

Lorsque l'utilisateur de l'objet (3) portable de communication sans contact, place ou passe son doigt sur le dispositif (1011) de reconnaissance d'empreinte digitale, un signal représentatif de l'empreinte captée, est transmis, par des premiers moyens de communication à des moyens de traitement du dispositif d'authentification, pour être comparé à un ou plusieurs codes autorisés. Si le résultat de la comparaison est valide, les moyens de traitement commandent, par des seconds moyens de communication, l'interrupteur (101) pour désactiver le dispositif (1) de

protection pendant une durée déterminée, par exemple, de manière non limitative, de 1 seconde à 1 minute, cette durée permettant d'effectuer la transaction sans contact.

Selon une variante de réalisation, comme représenté à la figure 7, le dispositif de sécurisation est désactivé par un dispositif (1012, 1014, 1013) d'authentification par reconnaissance visuelle, par exemple de l'iris. Le lecteur d'iris comprend par exemple une caméra numérique équipée d'un objectif de type macro, associée à un moyen d'éclairage de l'iris disposé proche de l'œil.

Le dispositif d'authentification comporte par exemple un dispositif de reconnaissance de l'iris fixé sur des lunettes (1013) ou un autre support, porté par l'utilisateur, et relié par un câble (1014) de communication avec un circuit (1012) de traitement qui active ou désactive l'interrupteur (101). Lorsque l'utilisateur de l'objet (3) portable de communication sans contact, place le lecteur d'iris devant son œil, un signal représentatif de l'empreinte d'iris, est transmis, par des premiers moyens de communication à des moyens de traitement du dispositif d'authentification, pour être comparé à un ou plusieurs codes autorisés. Si le résultat de la comparaison est valide, les moyens de traitement commandent l'interrupteur (101), par des seconds moyens de communication, pour désactiver le dispositif (1) de protection.

Selon un autre exemple de réalisation, comme représenté à la figure 8, le dispositif (1) de sécurisation est désactivé par un dispositif (1011) d'authentification par reconnaissance vocale comportant un microphone (1017) relié par un câble (1016) de communication à un circuit de traitement (1015). Lorsque l'utilisateur de l'objet portable de communication sans contact prononce un message clé audio dans le microphone, un signal représentatif du message audio est transmis par le câble (1016) au circuit (1015) de traitement. Le circuit de traitement comprend des moyens d'analyser ce signal représentatif du message audio et commande la désactivation du dispositif (1) de protection si le message audio est authentifié. L'authentification comprend par exemple une comparaison du

signal représentatif du message audio prononcé avec un ou plusieurs signaux autorisés mémorisés.

Dans le cas où l'authentification échoue, l'interrupteur (101) reste dans un état stable d'autorisation du fonctionnement du dispositif (1) de protection. De manière non limitative, si l'authentification réussit, les moyens de traitement commandent l'ouverture de l'interrupteur (101) pendant une durée déterminée, comprise par exemple entre 1 seconde et 1 minute, puis retournent dans un état stable de commande de la fermeture de l'interrupteur (101) pour activer le dispositif de sécurisation.

Il doit être évident pour les personnes versées dans l'art que la présente invention permet des modes de réalisation sous de nombreuses autres formes spécifiques sans l'éloigner du domaine d'application de l'invention comme revendiqué. Par conséquent, les présents modes de réalisation doivent être considérés à titre d'illustration, mais peuvent être modifiés dans le domaine défini par la portée des revendications jointes, et l'invention ne doit pas être limitée aux détails donnés ci-dessus.

REVENDICATIONS

1. Dispositif de protection pour objet (3) de communication sans contact à circuit (31, 32) intelligent mémorisant des informations sensibles ou des informations donnant accès à des services, caractérisé en ce que le dispositif (1) de protection comprend au moins des moyens (13) de réception radio de premiers signaux (S22) radio émis par une borne (2) ou un lecteur sans contact, dans une plage de fréquences de l'ordre du mégahertz à quelques dizaines de mégahertz, les premiers signaux (S22) reçus générant l'énergie de fonctionnement du dispositif (1) de protection pour activer un circuit (11) intelligent du dispositif (1) de protection générateur d'un signal (f) de brouillage à émettre par des moyens (14) d'émission du dispositif de sécurisation sous la forme d'ondes (S21) radio de brouillage destinées à la borne (2) ou au lecteur, les ondes (S21) radio de brouillage étant produites à la réception des premiers signaux avec une puissance suffisante pour être reçues par des moyens de réception radio de la borne (2) ou du lecteur et détériorer la réception par les moyens de réception radio de la borne (2) ou du lecteur de seconds signaux radio émis par l'objet (3) de communication sans contact, en réponse à l'activation par la borne (2) ou le lecteur, et des moyens (12) d'interruption pour valider ou invalider le dispositif (1) de protection.

2. Dispositif de protection selon la revendication 1, caractérisé en ce que l'objet (3) de communication sans contact, protégé par le dispositif (1) de protection, est activé dans un domaine (20) de portée de la borne (2) ou du lecteur, la borne ou le lecteur, émettant les premiers signaux (S22) radio par des moyens d'émission radio, pour communiquer avec l'objet (3) de communication sans contact et alimenter l'objet de communication sans contact, en énergie par des moyens (33) de réception radio de l'objet de communication sans contact,

l'objet (3) de communication sans contact émettant les seconds signaux radio, par des moyens (33) d'émission radio de l'objet de communication sans contact, pour communiquer avec la borne (2) ou le lecteur, par les moyens de réception radio de la borne ou du lecteur.

3. Dispositif de protection selon la revendication 2, caractérisé en ce que les moyens (33) de réception radio de l'objet de communication sans contact et les moyens (13) de réception radio du dispositif (1) de protection comprennent chacun une bobine (102) appartenant à un circuit (108) résonnant accordé déterminé.

4. Dispositif de protection selon la revendication 3, caractérisé en ce que les moyens (33) d'émission radio de l'objet de communication sans contact et les moyens (14) d'émission radio du dispositif (1) de protection comprennent chacun la bobine (102) dans le circuit (108) résonnant accordé utilisé pour la réception radio.

5. Dispositif de protection selon une des revendications 2 à 4, caractérisé en ce que la communication, entre d'une part la borne ou le lecteur et d'autre part l'objet de communication sans contact, étant réalisée selon un protocole anti-collision déterminé, l'objet de communication sans contact émettant les seconds signaux radio en réponse aux premiers signaux radio après au moins après l'émission d'une requête par les premiers signaux, le circuit (11) intelligent du dispositif (1) de protection commande une émission des ondes (S21) radio de brouillage en réponse aux premiers signaux radio, l'émission des ondes radio de brouillage se maintenant durant la réception des premiers signaux.

6. Dispositif de protection selon la revendication 5, caractérisé en ce que le signal de brouillage, reçu par la borne (2) ou le lecteur, est représentatif de données déterminées traitées par des moyens de traitement de la borne ou du lecteur, pour provoquer une réinitialisation dans l'exécution du protocole anti-collision.

7. Dispositif de protection selon la revendication 5, caractérisé en ce que le signal de brouillage, reçu par la borne (2) ou le lecteur, est représentatif de données déterminées traitées par des moyens de traitement de la borne ou du lecteur pour provoquer une saturation des moyens de traitement.

8. Dispositif de protection selon une des revendications 1 à 7, caractérisé en ce que le signal de brouillage généré, lors de la réception des premiers signaux émis par la borne ou le lecteur, par le circuit intelligent du dispositif de protection, est un signal prédéterminé pour économiser l'énergie dépensée par le circuit (11) intelligent en faveur de l'énergie utilisée par les moyens (14) d'émission radio du dispositif (1) de protection.

9. Dispositif de protection selon la revendication 8, caractérisé en ce que le circuit (11) intelligent du dispositif de protection comprend un compteur diviseur de la fréquence de modulation des premiers signaux émis par la borne (2) ou le lecteur.

10. Dispositif de protection selon une des revendications 1 à 9, caractérisé en ce que des moyens interactifs du dispositif de protection comprennent un capteur biométrique transmettant à un circuit d'authentification du dispositif de protection, commandant les moyens d'interruption, une information représentative d'un paramètre biométrique mesuré, comparée avec au moins une information représentative d'un paramètre biométrique d'un utilisateur autorisé à utiliser l'objet (3) de communication sans contact.

11. Dispositif de protection selon une des revendications 1 à 9, caractérisé en ce que des moyens interactifs du dispositif de protection comprennent un clavier alphanumérique transmettant à un circuit d'authentification du dispositif de protection, commandant les moyens d'interruption, une information représentative d'un code entré par un utilisateur, comparé avec au moins un code d'autorisation de l'utilisation de l'objet (3) de communication sans contact.

12. Dispositif de protection selon une des revendications 1 à 9, caractérisé en ce que les moyens d'interruption comprennent un interrupteur ou un bouton poussoir disposé à la surface du dispositif de protection ou dans un logement en creux aménagé dans l'épaisseur du dispositif de protection.

13. Dispositif de protection selon une des revendications 1 à 9, caractérisé en ce que les moyens d'interruption comprennent un interrupteur ou un bouton poussoir disposé à l'extrémité d'une ligne de communication avec le dispositif de protection.

14. Système sécurisé portable de communication sans contact comprenant au moins un objet (3) de communication sans contact à circuit (31, 32) intelligent mémorisant des informations sensibles ou des informations donnant accès à des services, l'objet (3) de communication sans contact comprenant des moyens (33) de réception radio de signaux de communication et d'alimentation et des moyens (33) d'émission radio de signaux de communication, une première bobine déterminée dans un premier circuit résonnant accordé appartenant aux moyens (33) d'émission et de réception radio de l'objet (3) de communication sans contact, le système étant caractérisé en ce qu'il comporte au moins :

un dispositif (1) de protection comprenant des moyens (13) de réception radio de signaux de communication et d'alimentation, dans une plage de fréquences de l'ordre du mégahertz à quelques dizaines de mégahertz, pour activer un circuit (11) intelligent du dispositif de protection générateur d'un signal (f) de brouillage à émettre par des moyens (14) d'émission du dispositif de protection sous la forme d'ondes (S21) radio de brouillage, une seconde bobine (102) déterminée dans un second circuit (108) résonnant accordé appartenant aux moyens d'émission et de réception radio du dispositif de protection, le dispositif de protection comprenant des moyens (12) d'interruption permettant de valider ou d'invalider le fonctionnement du dispositif de protection,

les moyens (12) d'interruption du circuit de brouillage étant commandés, selon le résultat d'une comparaison effectuée, par des moyens de comparaison entre d'une part une information provenant de moyens interactifs (1010, 1011, 1012, 1015) d'authentification et d'autre part une information mémorisée dans des moyens de mémorisation.

15. Système sécurisé selon la revendication 14, caractérisé en ce que le dispositif (1) de protection et l'objet de communication sans contact, sont rendus solidaires dans un boîtier à fermeture sécurisée, dont la fermeture valide le fonctionnement du dispositif de protection.

16. Système sécurisé selon la revendication 15, caractérisé en ce que le boîtier sécurisé est moulé d'un seul bloc autour du dispositif (1) de protection et de l'objet (3) de communication sans contact.

17. Système sécurisé selon la revendication 15, caractérisé en ce que le boîtier sécurisé est fermé autour du dispositif (1) de protection et de l'objet (3) de communication sans contact, l'ouverture du boîtier étant commandée par une clé sécurisée.

18. Système sécurisé selon une des revendications 15 à 17, caractérisé en ce que le boîtier sécurisé comporte un logement pour accueillir au moins un objet supplémentaire de communication sans contact mémorisant des informations sensibles ou des informations donnant accès à des services.

19. Système sécurisé selon une des revendications 14 à 18, caractérisé en ce que les moyens interactifs d'authentification comprennent un clavier alphanumérique transmettant aux moyens de comparaison, une information représentative d'un code entré par un utilisateur, comparé avec au moins un code d'autorisation de l'utilisation de l'objet (3) de communication sans contact.

20. Système sécurisé selon une des revendications 14 à 18, caractérisé en ce que les moyens interactifs d'authentification comprennent un capteur biométrique transmettant aux moyens de comparaison, une

information représentative d'un paramètre biométrique mesuré, comparée avec au moins une information représentative d'un paramètre biométrique d'un utilisateur autorisé à utiliser l'objet (3) de communication sans contact.

21. Système sécurisé selon la revendication 20, caractérisé en ce que le capteur biométrique est un capteur d'empreinte digitale.

22. Système sécurisé selon la revendication 21, caractérisé en ce que le capteur d'empreinte digitale est un lecteur optique devant lequel l'utilisateur passe son doigt.

23. Système sécurisé selon la revendication 20, caractérisé en ce que le capteur biométrique est un lecteur d'iris.

24. Système sécurisé selon la revendication 20, caractérisé en ce que le capteur biométrique est un analyseur d'empreinte vocale.

25. Système sécurisé selon une des revendications 19 à 24, caractérisé en ce que les moyens interactifs d'authentification et les moyens de comparaison comprennent des moyens d'alimentation pour réaliser la comparaison et commander les moyens d'interruption avant l'entrée du système sécurisé dans le domaine de portée.

26. Dispositif de protection d'au moins un objet de communication sans contact à circuit intelligent mémorisant des informations sensibles ou des informations donnant accès à des services, caractérisé en ce qu'il comprend au moins des moyens (13) de réception de signaux (S22) radio dans une plage de fréquences de l'ordre du mégahertz à quelques dizaines de mégahertz, les signaux (S22) radio reçus générant l'énergie de fonctionnement du dispositif (1) de protection pour activer un circuit (11) intelligent générateur d'un signal (f) de brouillage à émettre par des moyens (14) d'émission du dispositif de protection sous la forme d'ondes (S21) radio de brouillage, une bobine (102) déterminée dans un circuit (108) résonnant accordé appartenant aux moyens d'émission et de réception radio du dispositif (1) de protection, et des moyens (12) d'interruption validant ou invalidant le fonctionnement du dispositif de protection.

27. Dispositif de protection selon la revendication 26, caractérisé en ce que, le signal de brouillage est émis dès réception des premiers signaux avant la fin d'une requête conforme à un protocole de communication..

28. Dispositif de protection selon la revendication 26 ou 27, caractérisé en ce qu'au moins les moyens d'émission et de réception radio du dispositif de protection et le circuit intelligent du dispositif de protection sont insérés dans un boîtier de même dimensions que l'objet de communication sans contact à circuit intelligent protégé.

29. Dispositif de protection selon une des revendications 26 à 28, caractérisé en ce que les moyens d'interruption comprennent un interrupteur disposé à la surface du dispositif de protection ou dans un logement en creux aménagé dans l'épaisseur du dispositif de protection.

30. Dispositif de protection selon une des revendications 26 à 28, caractérisé en ce que les moyens d'interruption comprennent un interrupteur disposé à l'extrémité d'une ligne de communication avec le dispositif de protection.

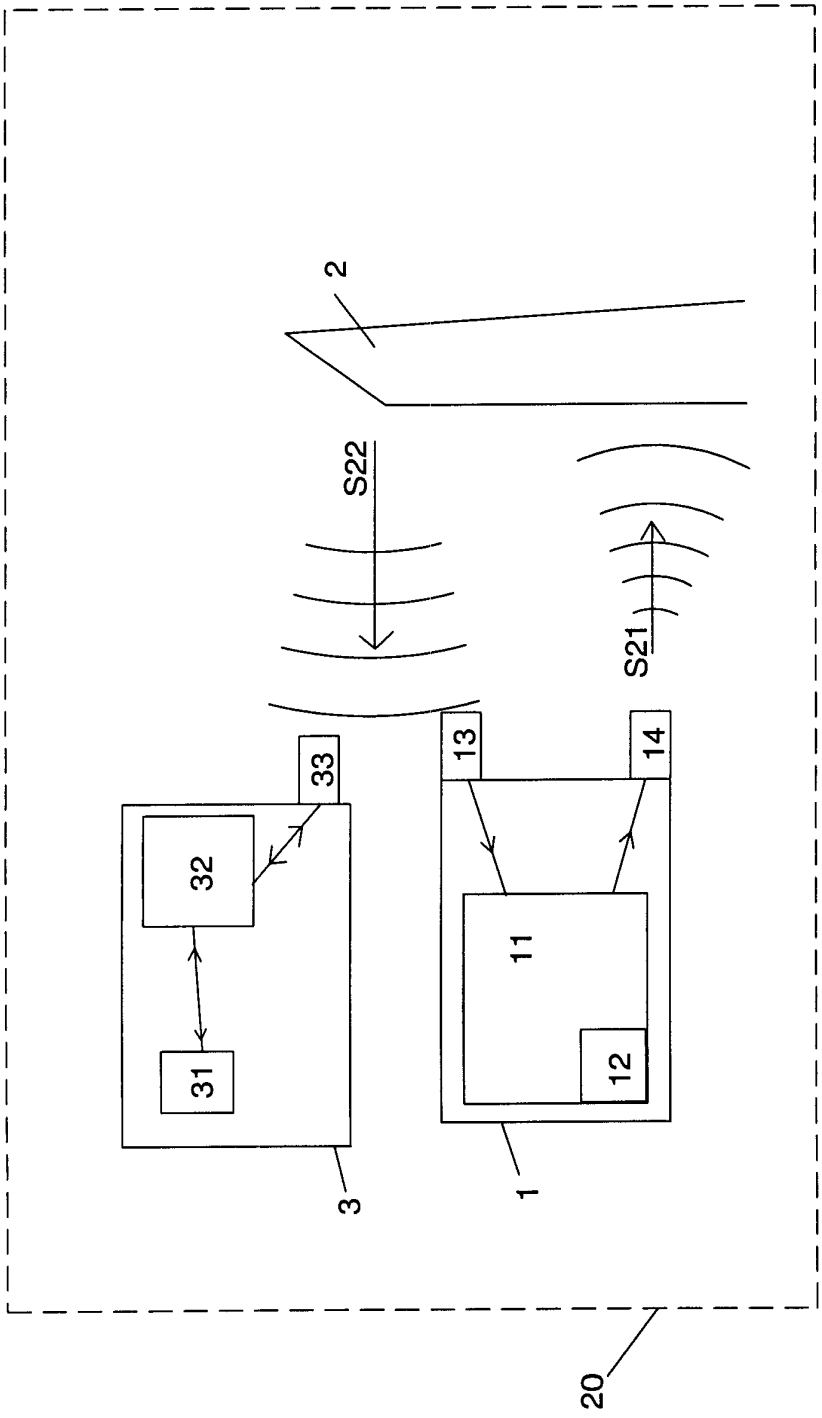
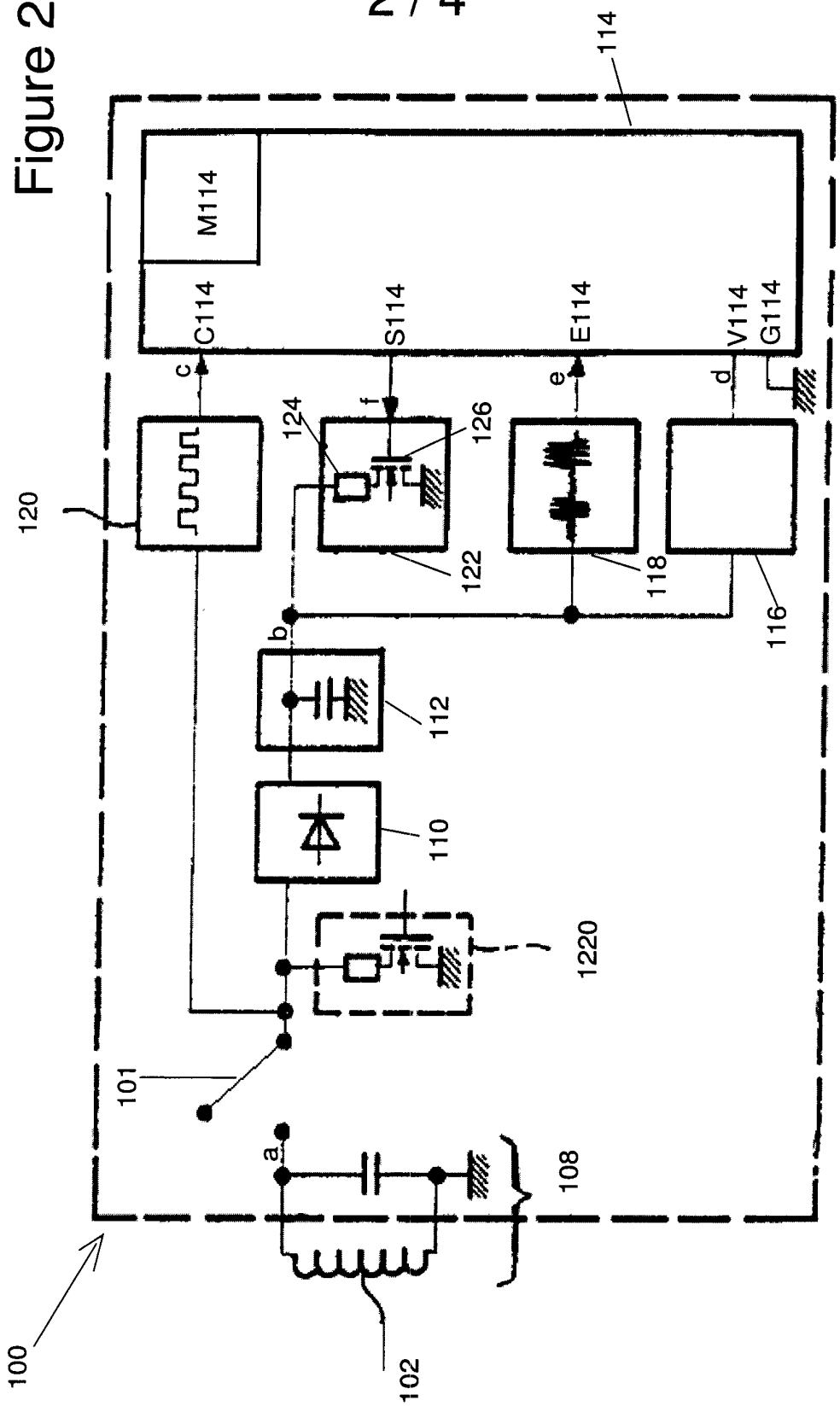


Figure 1

Figure 2


114
M114
C114
S114
E114
V114
G114
c
f
e
d
124
126
120
122
118
116
b
112
110
1220
101
a
108
100
102

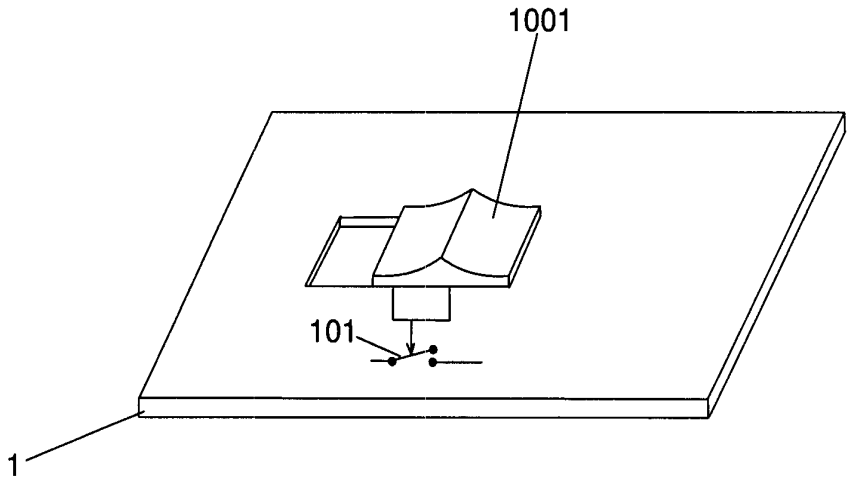


Figure 3

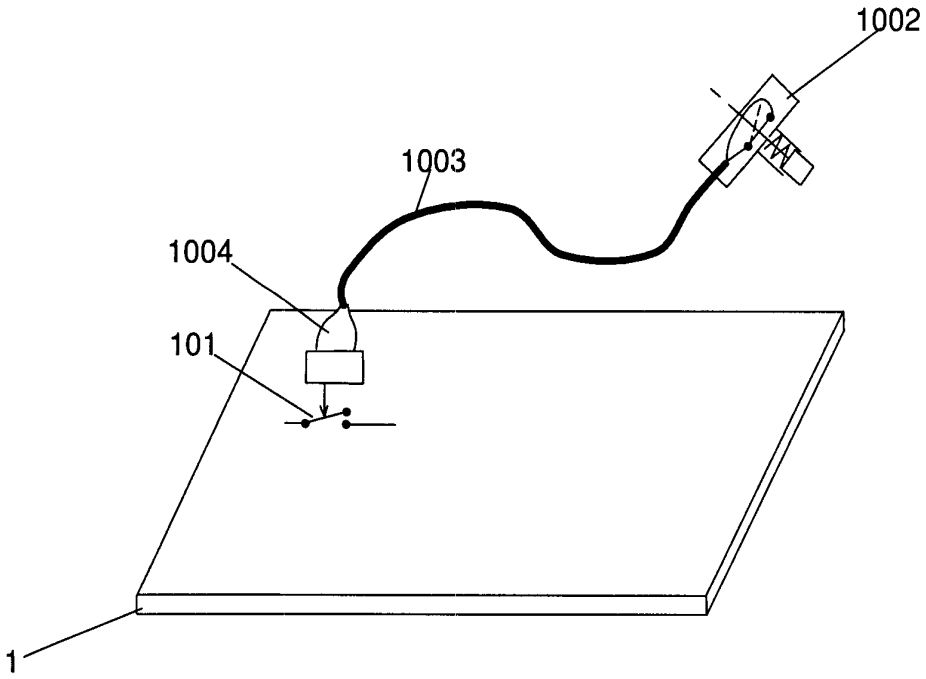


Figure 4

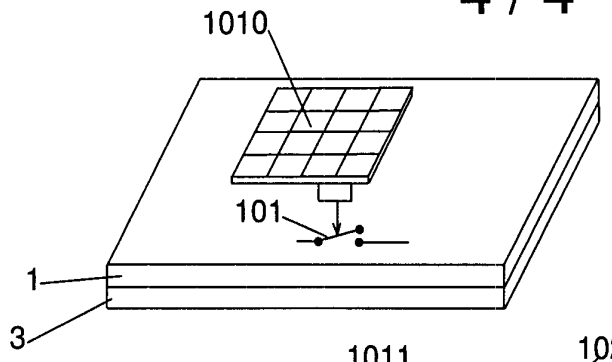


Figure 5

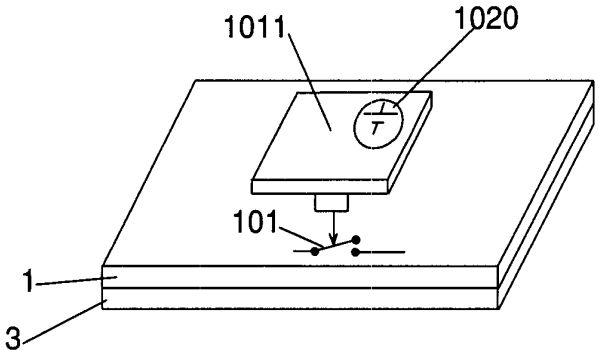


Figure 6

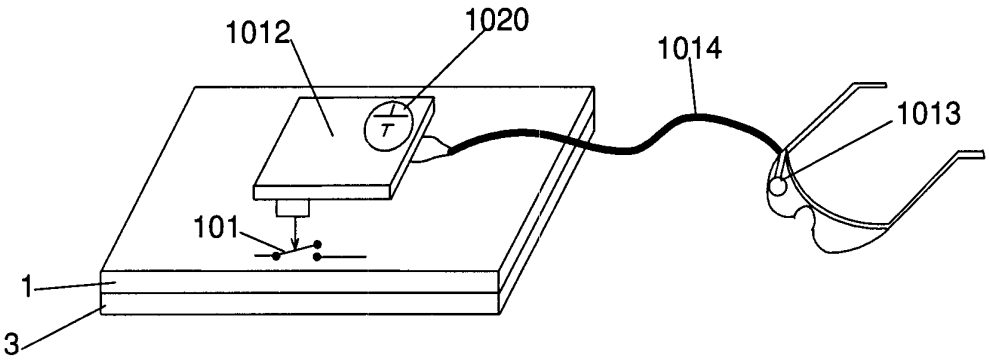


Figure 7

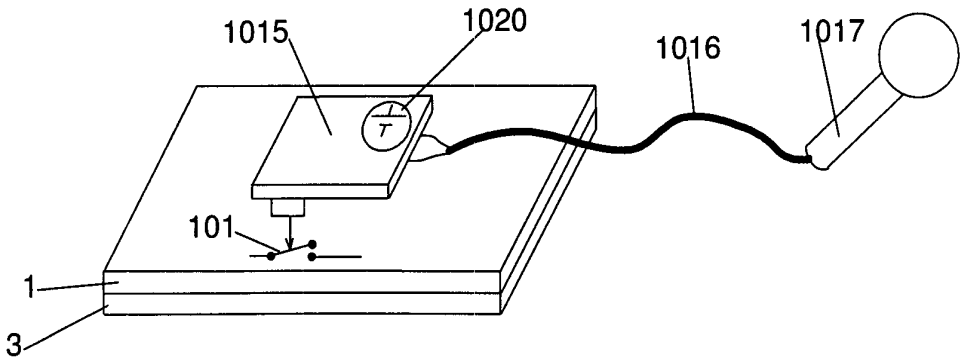


Figure 8

RÉPUBLIQUE FRANÇAISE

2908205

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 686830
FR 0609610

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 2005/052846 A (KONINKL PHILIPS ELECTRONICS NV [NL]; ARENDONK ANTON [NL]) 9 juin 2005 (2005-06-09)	1-13, 26-30	G06K19/073 G06K7/08 G06K9/00
A	* page 5, ligne 1 - page 10, ligne 10; figures 1-3 *	14-25	H04L9/32 G06F21/00

X	JUELS A ET AL ASSOCIATION FOR COMPUTING MACHINERY: "The Blocker Tag: Selective Blocking of RFID tags for Consumer Privacy" PROCEEDINGS OF THE 10TH. ACM CONFERENCE ON COMPUTER AND COMMUNICATIONSSECURITY. (CCS'03). WASHINGTON, DC, OCT. 27 - 31, 2003, ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, NEW YORK, NY : ACM, US, vol. CONF. 10, 27 octobre 2003 (2003-10-27), pages 103-111, XP002341165 ISBN: 1-58113-738-9	1-13, 26-30	
A	* le document en entier *	14-25	DOMAINES TECHNIQUES RECHERCHÉS (IPC)
	-----		G06K

Date d'achèvement de la recherche	Examinateur
10 juillet 2007	Degraeve, Alexis

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 0609610 FA 686830

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 10-07-2007
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 2005052846 A	09-06-2005	CN 1886750 A	27-12-2006
		JP 2007512611 T	17-05-2007
		US 2007075145 A1	05-04-2007

EPO FORM P0465