

①⑨ RÉPUBLIQUE FRANÇAISE
INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE
COURBEVOIE

①⑪ N° de publication :

3 059 122

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

②① N° d'enregistrement national :

16 01646

⑤① Int Cl⁸ : G 06 K 7/10 (2017.01), G 06 K 19/08, B 42 D 25/305

⑫

DEMANDE DE BREVET D'INVENTION

A1

②② Date de dépôt : 21.11.16.

③③ Priorité :

④③ Date de mise à la disposition du public de la
demande : 25.05.18 Bulletin 18/21.

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

⑥③ Références à d'autres documents nationaux
apparentés :

○ Demande(s) d'extension :

⑦① Demandeur(s) : IMPRIMERIE NATIONALE Société
anonyme — FR.

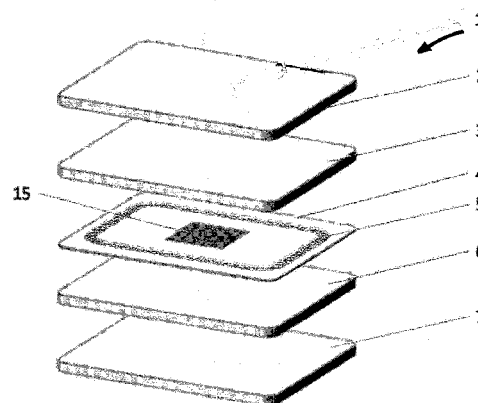
⑦② Inventeur(s) : COMBRET FABIEN, MEAR BENJA-
MIN et KAMBOURIAN HAIG.

⑦③ Titulaire(s) : IMPRIMERIE NATIONALE Société ano-
nyme.

⑦④ Mandataire(s) : GLOBAL INVENTIONS.

⑤④ DOCUMENT DE SECURITE POURVU D'UNE ANTENNE.

⑤⑦ L'invention concerne un système de vérification de
l'authenticité d'un document de sécurité (1), comprenant
d'une part un ensemble de documents de sécurité (1) asso-
ciés à des utilisateurs, et d'autre part des lecteurs (8) des-
tinés à vérifier l'authenticité desdits documents (1),
caractérisé en ce que chaque document de sécurité (1),
comporte une antenne passive (5) présentant au moins une pre-
mière fréquence de résonance (F_{0D}) constituant une
signature électromagnétique (16) dudit document, et en ce
que chaque lecteur (8) comporte une boucle de mesure (13)
apte à mesurer la signature électromagnétique d'un docu-
ment (1) lorsque celui-ci est approché du lecteur (8), et un
circuit électronique (9) pour comparer cette signature élec-
tromagnétique à une signature électromagnétique de réf-
érence (F_{0R}) mémorisée dans ledit lecteur (8) ou sur ledit
document de sécurité (1).



FR 3 059 122 - A1



Document de sécurité pourvu d'une antenne

L'invention concerne la sécurité des documents régaliens ou autres documents officiels, tels que les passeports, cartes d'identité, permis de conduire,
5 cartes grises automobiles, etc.

Etat de la technique

Dans l'état actuel de la technique, la sécurité des documents officiels dépourvus de circuits électroniques est conditionnée par la présence de motifs de
10 sécurité imprimés en surface du document, ou intégrés à l'une des couches constitutives du document.

Ainsi, on utilise des éléments tactiles imprimés en surface des documents, des motifs complexes tels que des guilloches, ou des hologrammes difficiles à reproduire. Pour vérifier l'authenticité de ce type de documents, il suffit alors
15 généralement d'un examen visuel.

D'autres documents officiels peuvent comporter des couches internes dans lesquelles on peut écrire des informations au moyen d'un faisceau laser. Dans ce cas la vérification de l'authenticité nécessite en général des moyens complémentaires, notamment d'éclairage, pour être en mesure de vérifier les
20 informations cachées à l'intérieur du document.

On connaît aussi des documents encore plus sécurisés, utilisant une puce microélectronique pour stocker des informations de sécurité codées et/ou cryptées. Dans les versions dites « sans contact » de ces documents, la puce est connectée à une antenne, de façon à permettre une communication
25 radiofréquence avec un lecteur externe sans contact.

Si les produits à puce sont susceptibles de présenter un niveau de sécurité plus important, ils sont aussi plus coûteux et plus complexes à fabriquer et à mettre en œuvre, ce qui ne convient pas à tous les marchés. En effet, certains marchés auraient besoin, pour des questions de coût, de documents moins
30 coûteux qu'un document à puce microélectronique, tout en présentant un niveau de sécurité supérieur aux documents simplement pourvus d'un motif de sécurité imprimé en surface, ou intégré dans l'épaisseur du document.

Buts de l'invention

Un but général de l'invention est par conséquent de proposer des documents de sécurité qui soient dépourvus des inconvénients précités.

5 Un autre but de l'invention est de proposer une solution technique permettant d'accroître la résistance des documents à la fraude, à moindre coût, c'est-à-dire même lorsqu'ils sont dépourvus d'une puce microélectronique.

Un autre but de l'invention est de proposer des documents dont l'authenticité puisse être vérifiée de façon efficace par une infrastructure simple et
10 peu coûteuse.

Résumé de l'invention

L'invention a par conséquent pour objet un système de vérification de l'authenticité d'un document de sécurité, comprenant d'une part un ensemble de
15 documents de sécurité associés à des utilisateurs, et d'autre part des lecteurs destinés à vérifier l'authenticité desdits documents, caractérisé en ce que chaque document de sécurité comporte une antenne passive présentant au moins une première fréquence de résonance (F_{0D}) constituant une signature électromagnétique dudit document, et en ce que chaque lecteur comporte une
20 boucle de mesure apte à mesurer la signature électromagnétique d'un document lorsque celui-ci est approché du lecteur, et un circuit électronique pour comparer cette signature électromagnétique à une signature électromagnétique de référence (F_{0R}) mémorisée dans ledit lecteur ou sur ledit document.

Ainsi, lorsque la comparaison est positive, le vérificateur utilisant le système
25 a une indication fiable et sûre que le document présenté au lecteur est un document authentique.

Selon un mode de réalisation avantageux de l'invention, chaque lecteur du système comporte en outre une antenne passive rapportée ou intégrée, présentant une seconde fréquence de résonance (F_{0L}) de sorte que lorsque l'antenne passive
30 du document et l'antenne passive du lecteur sont couplées entre elles, elles présentent une fréquence de résonance complexe F_{0LD} présentant plusieurs pics

de résonance et constituant une signature électromagnétique complexe dudit document.

Selon l'invention, chaque lecteur comporte des moyens de signalisation pour indiquer, en fonction du résultat de la comparaison effectuée par le lecteur, le fait
5 que le document de sécurité présenté est un document authentique, et dans le cas contraire, le fait que le document présenté est un faux.

Avantageusement, lesdits moyens de signalisation sont des moyens d'affichage lumineux de type LED, ou des moyens sonores.

Dans une version encore plus sûre du système selon l'invention, chaque
10 document comporte, en plus de son antenne passive ayant une fréquence de résonance (F_{OD}), une représentation graphique codée de ladite fréquence de résonance (F_{OD}), et chaque lecteur comporte en outre un capteur optique et un microcontrôleur pour lire et pour décoder ladite représentation graphique.

La représentation graphique de la fréquence de résonance (F_{OD}) des
15 documents est par exemple un QR code.

Dans un mode de réalisation avantageux des documents du système, les pistes de l'antenne passive des documents et le QR code sont réalisés sur une seule et même couche métallique intégrée dans l'épaisseur du document, et protégés par des couches externes.

20 D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description détaillée et des dessins annexés dans lesquels :

- la figure 1 représente une vue en perspective éclatée d'un document selon l'invention, au format d'une carte;
- la figure 2 représente un lecteur de carte sous forme schématique ;
- 25 - la figure 3 représente la réponse en fréquence du lecteur seul, équipé d'une antenne, la réponse en fréquence d'une carte seule selon l'invention, équipée d'une antenne, et la réponse en fréquence du système constitué par le lecteur de la figure 2 et par la carte de la figure 1 ;
- la figure 4 représente une variante de carte selon l'invention, pourvue
30 d'une antenne et d'un QR code ;
- la figure 5 représente un organigramme fonctionnel du logiciel de test exécuté par le lecteur pour le test de cartes selon la figure 1, sans QR code ;

- la figure 6 représente un organigramme fonctionnel du logiciel de test exécuté par le lecteur pour le test de cartes selon la figure 4, avec un QR code sur les cartes testées.

5 **Description détaillée**

On a représenté en figure 1 un document de sécurité 1, au format d'une carte en matière plastique ayant des dimensions conformes à la norme ISO 7816-1. Bien entendu ce facteur de forme n'est qu'un exemple pratique, le facteur de forme
10 du document n'est absolument pas limitatif de la portée de l'invention.

La plupart des documents de sécurité existants sont des cartes en matière plastique comportant simplement sur les couches externes des informations imprimées relatives à l'émetteur de la carte, et des informations graphiques relatives au titulaire de la carte, pour son identification. Les informations de la carte
15 sont destinées à être lues soit par un contrôleur humain, soit par un dispositif d'acquisition de type scanner connecté à un système de numérisation et de traitement des informations lues. Dans ce contexte, ces cartes sont très simples et ne comportent ni puce microélectronique, ni antenne.

Le principe de l'invention consiste au contraire à doter les documents de
20 sécurité, par exemple les cartes 1 telles que celle de la figure 1, d'une antenne passive 5 prévue pour interagir avec une antenne d'un lecteur de carte. L'antenne 5 de la carte n'est pas quelconque, elle est choisie pour présenter une certaine signature électromagnétique particulière, notamment une fréquence de résonance particulière et calibrée.

25 Pour la suite de l'exposé, on considérera que la signature électromagnétique d'une antenne est représentée de façon simplifiée par sa fréquence de résonance. On associera donc une fréquence de résonance donnée à un type de carte donné. Ainsi, toutes les cartes ou documents émis par une autorité donnée, auront une fréquence de résonance unique propre.

30 Dans une version de base de l'invention, les lecteurs de carte du système, tel que le lecteur 8 schématisé en figure 2, seront équipés d'un microcontrôleur 9 pourvu d'une mémoire (non représentée) dans laquelle est stockée une valeur de

fréquence de résonance de référence notée F_{OR} , correspondant à celle des documents authentiques utilisés dans le système. Les lecteurs 8 comportent en outre une bobine de mesure 13 de la fréquence de résonance d'un document 1 qu'un utilisateur approchera du lecteur. La mesure de la fréquence de résonance de l'antenne 5 du document 1 est transmise dans le microcontrôleur 8 à un circuit de comparaison de la fréquence de résonance détectée à partir de la carte avec la fréquence de résonance de référence F_{OR} stockée en mémoire. Enfin, les lecteurs 8 comportent des moyens de signalisation (optiques, sonores, etc.), comme par exemple les LED 11, 12, pour signaler le résultat de la comparaison à l'utilisateur du système et lui indiquer qu'un document testé donné correspond à un document authentique ou à un document falsifié.

On comprend donc aisément que l'antenne spécifique 5 intégrée dans chaque document 1 augmente la résistance du document à la falsification, puisqu'un fraudeur devra avoir les moyens d'équiper à posteriori un faux document, avec une antenne présentant la même signature électromagnétique, en particulier la même fréquence de résonance, que les documents authentiques.

Mais l'intégration d'une telle antenne 5 dans un document reste à la portée de réseaux de fraudeurs structurés et équipés de matériel pour copier des antennes.

Il faut donc aller plus loin.

A cet effet, une version un peu plus avancée de l'invention prévoit d'équiper également les lecteurs 8 d'une antenne passive spécifique 14, encore appelée antenne de de-tuning, ayant sa propre fréquence de résonance caractéristique. Dans ce cas, lorsqu'on approche du lecteur 8 un document 1 conforme à l'invention et pourvu de sa propre antenne 5, on obtient un système de deux antennes 5, 14 couplées entre elles, et présentant une signature électromagnétique complexe 17, comme représenté en figure 3, comportant en particulier deux ou davantage de pics de résonance qui peuvent être détectés par la bobine de mesure 13 du lecteur.

Comme représenté en figure 3, supposons que l'antenne 14 du lecteur 8 ait une fréquence de résonance 16 un peu inférieure à 13 Mhz, et que l'antenne 5 du document 1 ait une fréquence de résonance 17 un peu supérieure à 13 Mhz. Alors le système d'antennes 5, 14 couplées entre elles aura une signature

électromagnétique propre 18, présentant deux pics de résonance, par exemple au voisinage de 11 et 16 Mhz.

A nouveau, la signature électromagnétique attendue de la paire d'antennes 5, 14 est stockée en mémoire du lecteur 8, et pour chaque nouveau document
5 approché du lecteur, celui-ci comparera la signature électromagnétique mémorisée, avec la signature électromagnétique détectée pour le système constitué par l'antenne passive 14 du lecteur couplée avec l'antenne passive 5 du nouveau document à tester.

Comme la signature électromagnétique 18 du système d'antennes 5, 14 est
10 plus complexe que dans le cas précédent avec une seule antenne 5 située sur le document, il devient plus difficile à répliquer de façon frauduleuse, mais cela reste possible avec les moyens appropriés.

Dans une version encore un peu plus sûre du système selon l'invention, les documents 1 et les lecteurs 8 sont encore équipés comme précédemment
15 d'antennes 5, 14 spécifiques, mais on ajoute en plus dans le lecteur un organe de traitement mathématique secret permettant de complexifier encore davantage la signature électromagnétique du système d'antennes constitué par l'antenne passive 14 du lecteur couplée avec l'antenne passive 5 d'un document.

Par exemple, le logiciel du lecteur calculera une fréquence de résonance
20 fictive F_{of} par un traitement du type :

$F_{of} = A.F_{OL} + B.F_{OD}$ où A et B sont des paramètres entiers ou non, et F_{OL} et F_{OD} représentent respectivement la fréquence de résonance de l'antenne passive 14 du lecteur, et la fréquence de résonance de l'antenne passive 5 du document.

Bien entendu le même traitement aura été appliqué préalablement aux
25 fréquences de résonance de référence du lecteur et d'un document authentique, pour pouvoir stocker en mémoire la valeur cible attendue.

Comme on le voit, pour pouvoir obtenir un document falsifié présentant la bonne signature électromagnétique 17, en particulier les bonnes fréquences de résonance, il faudra maintenant disposer de la fréquence de résonance 16 du
30 lecteur 8, de celle 17 d'un document authentique 5, et des paramètres A,B de l'opération secrète réalisée dans le lecteur.

Selon une variante préférée et encore plus sûre de l'invention, chaque document de sécurité 1 pourvu de son antenne 5, comportera, comme représenté en figure 4, une représentation graphique codée 15 de la signature électromagnétique de son antenne 5, en particulier de sa fréquence de résonance 16. Et chaque lecteur 8 sera équipé de moyens pour lire cette représentation graphique codée lorsque le document 1 est approché du lecteur 8, pour la décoder et pour la comparer à la fréquence de résonance de référence 17 attendue et stockée en mémoire du lecteur. Dans ce cas de figure, on peut se passer d'une antenne passive 14 sur chaque lecteur, mais les lecteurs devront comporter, 10 comme schématisé en figure 2, un capteur optique 10 pour lire la représentation graphique codée 15 disposée sur la carte.

En pratique, la représentation graphique codée 15 de la valeur de la fréquence de résonance de l'antenne d'un document sera par exemple constituée par un QR code imprimé sur l'une des couches 2, 3, 4, 6, 7 de la carte. Ce genre de 15 code est très difficile à répliquer. Mais d'autres représentations graphiques codées, comme notamment les codes à barre 2D, sont envisageables.

Selon la localisation du QR code ou équivalent, il pourra être utile que les couches de matière plastique situées au-dessus du QR code soient transparentes, ou comportent une fenêtre transparente, pour faciliter la lecture du QR code par le 20 capteur optique 10 du lecteur 8.

Afin d'augmenter encore davantage la sécurité du système, les valeurs de fréquence de résonance stockées dans un QR Code peuvent être assorties d'une protection numérique en authenticité, en intégrité ou en confidentialité. Par exemple, pour l'authenticité et l'intégrité, les données intégrées au QR code sont 25 préalablement signées numériquement grâce à une clé privée asymétrique fournie par l'émetteur du document. Pour vérifier la signature, il faut obtenir le certificat à clé publique correspondant de la part de l'entité qui a généré et certifié la clé asymétrique.

Pour la confidentialité, les données sont chiffrées avec une clé symétrique 30 fournie par l'émetteur du document. Pour déchiffrer le QR Code, il faut utiliser la clé symétrique qui est distribuée, comme cela est bien connu dans l'état de la technique.

Dans un mode de réalisation avantageux de l'invention, les pistes de l'antenne 5 du document 1 et le QR code 15 seront réalisés sur une seule et même couche métallique intégrée dans l'épaisseur du document lors de la fabrication de celui-ci. Ainsi toute manipulation de l'antenne 5 et du QR code 15 deviendra visible.

5 De préférence, le lecteur comporte des moyens de signalisation visuels ou sonores du résultat de la comparaison entre la valeur de la fréquence de résonance du document testé et la valeur de référence stockée dans le lecteur. Ces moyens prennent par exemple la forme d'une LED verte 11 pour signaler que le document présenté est authentique, et une LED rouge 12 pour signaler que le document
10 présenté est un faux.

En figure 5 on a représenté l'organigramme fonctionnel du logiciel de test des lecteurs 8 dans le cas où les documents testés 1 ne comportent pas de représentation graphique codée de leur fréquence de résonance. Dans ce cas, le lecteur 8 se met dans une boucle d'attente 20 d'une carte à tester, puis lorsqu'une
15 carte 1 arrive à proximité du lecteur 8, le lecteur mesure sa fréquence de résonance F_0 , puis en 22 lit l'empreinte électromagnétique de référence F_{OR} stockée en mémoire du lecteur. En 23, le microcontrôleur 9 du lecteur 8 compare la fréquence de résonance mesurée, à la fréquence de résonance de référence stockée en mémoire. En cas d'égalité des deux fréquences de résonance, le document 1
20 présenté est réputé authentique, ce qui est par exemple signalé en 24 par l'allumage de la LED verte. Dans le cas contraire, le document 1 présenté est réputé non authentique, ce qui est par exemple signalé en 25 par l'allumage de la LED rouge.

En figure 6 on a représenté l'organigramme fonctionnel du logiciel de test
25 des lecteurs 8 dans le cas où les documents testés comportent à la fois plusieurs fréquences de résonance F_0 , F_0' , F_0'' et une représentation graphique de ces fréquences de résonance, comme par exemple un QR code. La signature électromagnétique de référence stockée dans la mémoire du lecteur est alors par exemple la somme $F_0 + F_0' + F_0''$ des fréquences de résonances des cartes
30 authentiques, et cette signature est stockée, lors de la fabrication de la carte, à la fois dans la représentation graphique comme le QR code, et dans la mémoire du lecteur 8.

Ainsi, pour vérifier l'authenticité d'un document ou d'une carte approchée en 20 du lecteur, le lecteur mesure en 21 la ou les fréquences de résonance du document à tester, puis en 26 il lit le QR code ou équivalent situé sur le document, il calcule en 27 la somme des fréquences de résonance mesurées, et en 28 il
5 compare la somme calculée au QR code lu et éventuellement à la signature stockée en mémoire du lecteur 8. En cas de correspondance de tous les éléments, la carte est réputée authentique et la LED verte est allumée en 24, dans le cas contraire la LED rouge est allumée en 25.

Il est à noter que dans le cas où un QR code est utilisé, le lecteur n'a pas
10 nécessairement besoin d'être équipé d'une antenne de dé-tuning 14, puisque le niveau de sécurité obtenu grâce à l'usage d'un QR code est suffisant.

Avantages de l'invention

15 L'invention répond aux buts fixés. Grâce à l'invention, il est possible de vérifier simplement l'authenticité d'un document régalien, alors que les moyens de sécurité mis en œuvre représentent un coût minime.

En outre, la solution de l'invention présente une grande flexibilité, puisque les cartes peuvent être personnalisées par pays (une fréquence de résonance par
20 pays par exemple) ou par client. Le choix de la fréquence de résonance de la carte peut se faire au dernier moment lors du processus de fabrication de la carte, par usinage laser des pistes de l'antenne.

La sécurité est accrue par rapport à un document régalien sans puce ne comportant que des moyens de sécurité classiques: pour espérer contrefaire le
25 document selon l'invention, des connaissances de niveau laboratoire sont nécessaires.

En outre, toute tentative de désactiver la sécurité, par exemple en coupant ou en modifiant l'antenne de la carte ou en supprimant le QR code, laissera des traces visibles sur la carte.

30 Enfin, la durée de vie du document de sécurité est très longue, puisque les moyens supplémentaires sont constitués par une simple antenne facile à intégrer, sans module électronique.

La technique de l'invention pourrait également être adaptée comme sécurité complémentaire pour des documents à puce, même si dans ce cas on n'obtiendrait pas une sécurité aussi économique que dans le cas des documents ou cartes sans puce.

REVENDEICATIONS

1 – Système de vérification de l'authenticité d'un document de sécurité (1),
5 comprenant d'une part un ensemble de documents de sécurité (1) associés à des
utilisateurs, et d'autre part des lecteurs (8) destinés à vérifier l'authenticité desdits
documents (1), caractérisé en ce que chaque document de sécurité (1) comporte
une antenne passive (5) présentant au moins une première fréquence de résonance
(F_{0D}) constituant une signature électromagnétique (16) dudit document, et en ce
10 que chaque lecteur (8) comporte une boucle de mesure (13) apte à mesurer la
signature électromagnétique d'un document (1) lorsque celui-ci est approché du
lecteur (8), et un circuit électronique (9) pour comparer cette signature
électromagnétique à une signature électromagnétique de référence (F_{0R})
mémorisée dans ledit lecteur (8) ou sur ledit document de sécurité (1).

15

2 – Système de vérification selon la revendication 1, caractérisé en ce que
chaque lecteur (8) comporte en outre une antenne passive (14) présentant une
seconde fréquence de résonance (17) de sorte que lorsque l'antenne passive (5) du
document (1) et l'antenne passive (14) du lecteur (8) sont couplées entre elles,
20 elles présentent une fréquence de résonance complexe (18) présentant plusieurs
pics de résonance et constituant une signature électromagnétique dudit document.

3 – Système selon la revendication 1 ou la revendication 2, caractérisé en ce
que chaque lecteur (8) comporte des moyens de signalisation (11,12) pour
25 indiquer, en fonction du résultat de la comparaison effectuée par le lecteur (8), le
fait que le document de sécurité (1) présenté est un document authentique, et
dans le cas contraire, le fait que le document présenté est un faux.

4 – Système selon la revendication 3, caractérisé en ce que lesdits moyens
30 de signalisation sont des moyens d'affichage lumineux de type LED (11,12), ou des
moyens sonores.

5 – Système selon l'une quelconque des revendications précédentes, caractérisé en ce que chaque document de sécurité (1) comporte, en plus de son antenne passive (5) ayant une fréquence de résonance (F_{OD}), une représentation graphique codée (15) de ladite fréquence de résonance (F_{OD}), et en ce que chaque
5 lecteur (8) comporte en outre un capteur optique (10) et un microcontrôleur (9) pour lire et pour décoder ladite représentation graphique (15).

6 - Système selon la revendication 5, caractérisé en ce que ladite représentation graphique (15) de la fréquence de résonance (F_{OD}) des documents
10 est un QR code.

7 – Système selon la revendication 6, caractérisé en ce que les pistes de l'antenne passive ((5) du document (1) et le QR code sont réalisés sur une seule et même couche métallique intégrée dans l'épaisseur du document.

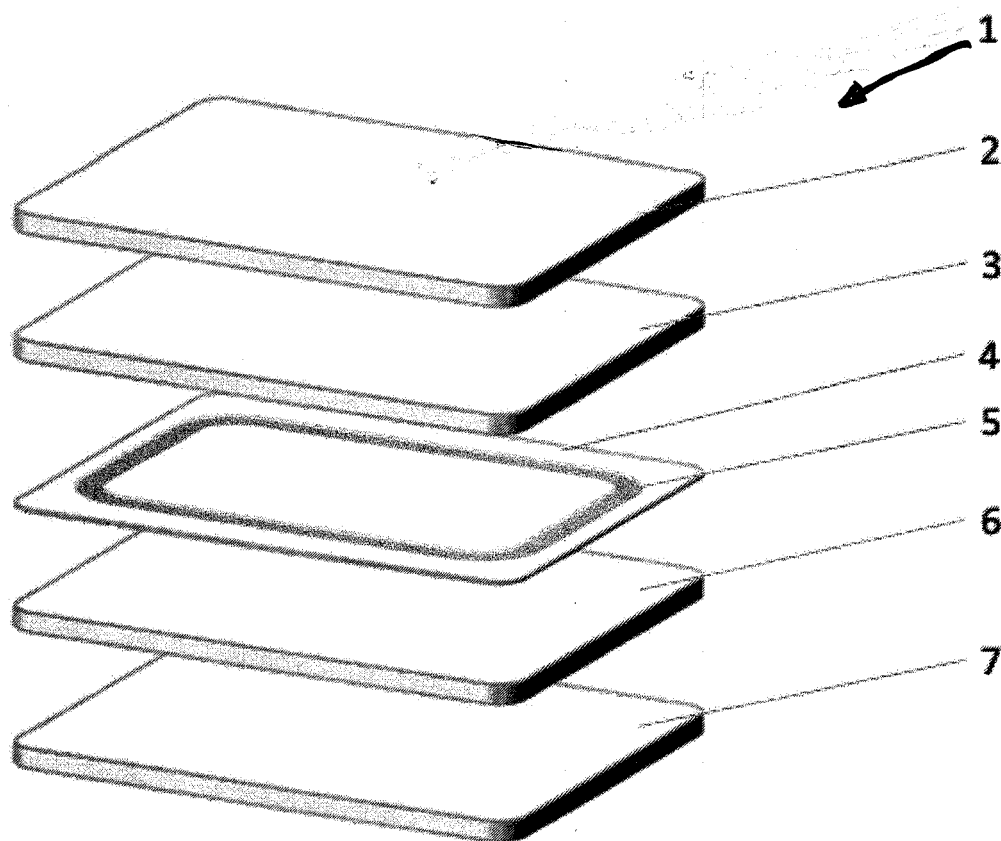
15

8 – Système selon l'une des revendications 5 à 7, caractérisé en ce que la représentation graphique codée (15) intègre une protection numérique en authenticité, en intégrité ou en confidentialité.

20

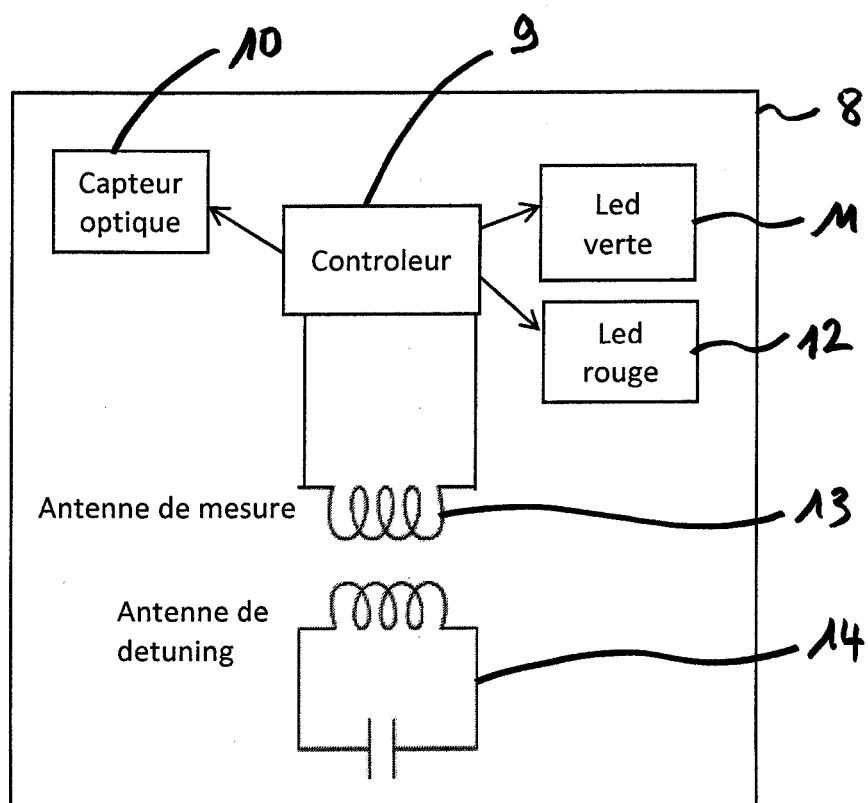
1/4

FIGURE 1



2/4

FIGURE 2



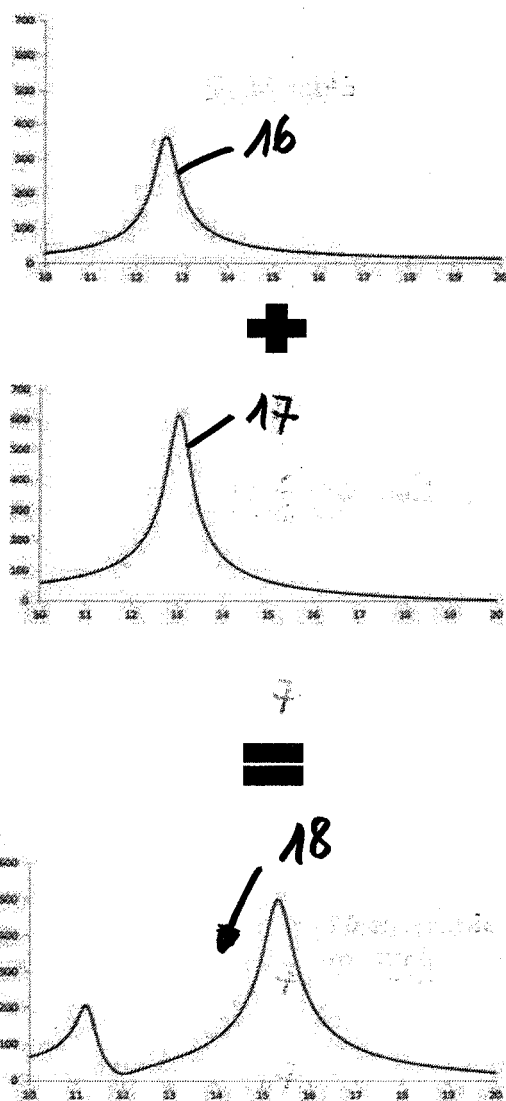
$\frac{3}{4}$ 

FIGURE 3

4/4

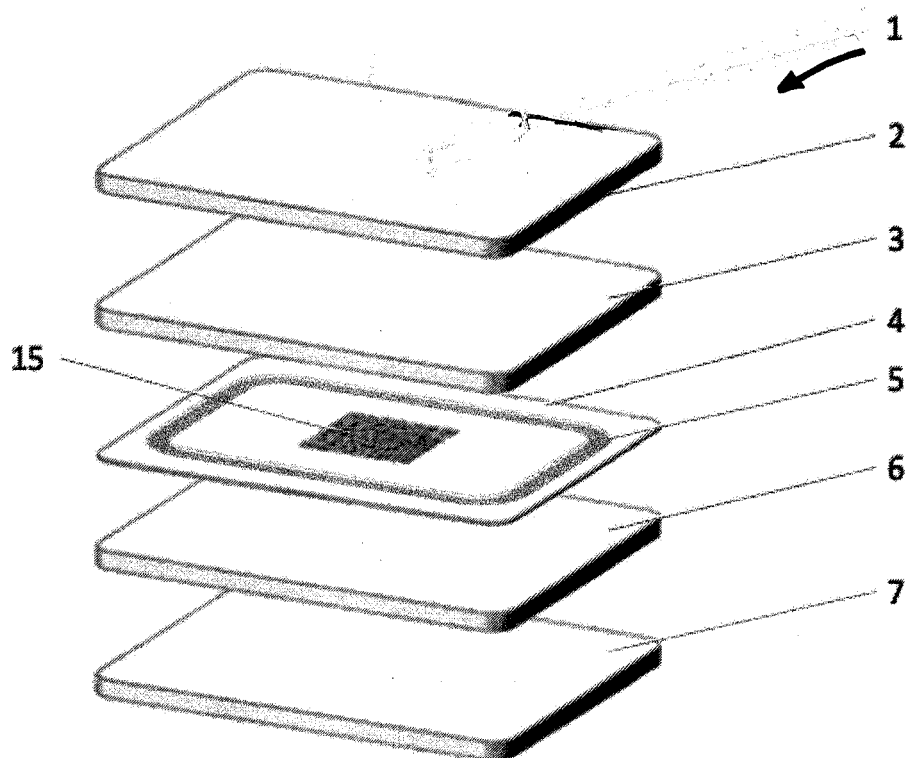


FIGURE 4

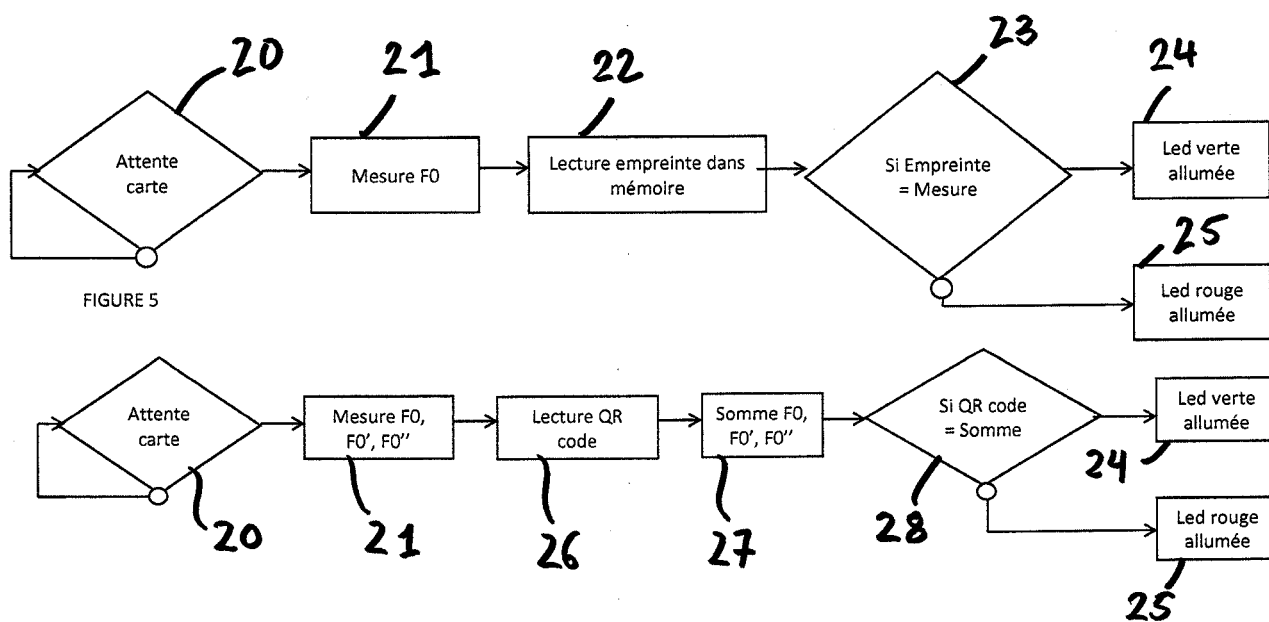


FIGURE 6



RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement
national

FA 834542
FR 1601646

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 2007/072251 A2 (KONINKL PHILIPS ELECTRONICS NV [NL]; WOLTERS ROBERTUS A M [NL]; JOHNSO) 28 juin 2007 (2007-06-28) * figure 1 * * page 9, ligne 16 - page 10, ligne 21 * * page 14, ligne 24 - page 15, ligne 8 * -----	1,3-8	G06K7/10 G06K19/08 B42D25/305
X	US 2005/225077 A1 (EICHENBERGER MARTIN [CH]) 13 octobre 2005 (2005-10-13) * figure 1 * * alinéas [0020], [0022] - [0025], [0029], [0032] * -----	1	
A	WO 2009/126999 A1 (UNIV MONASH [AU]; PRERADOVIC STEVAN [AU]; KARMAKAR NEMAI CHANDRA [AU];) 22 octobre 2009 (2009-10-22) * figure 1 * * page 9, ligne 25 - page 11, ligne 17 * -----	1-8	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			G06K
Date d'achèvement de la recherche		Examineur	
1 septembre 2017		Nicolle, Elsa	
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	

**ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE
RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1601646 FA 834542**

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 **01-09-2017**

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 2007072251 A2	28-06-2007	CN	101341518 A	07-01-2009
		EP	1966768 A2	10-09-2008
		JP	2009521040 A	28-05-2009
		TW	200732972 A	01-09-2007
		US	2008314715 A1	25-12-2008
		WO	2007072251 A2	28-06-2007

US 2005225077 A1	13-10-2005	AU	2003215834 A1	11-11-2003
		BR	PI0309970 A2	11-10-2016
		CA	2487780 A1	20-11-2003
		CN	1666224 A	07-09-2005
		EP	1363233 A1	19-11-2003
		EP	1504410 A1	09-02-2005
		JP	2005525255 A	25-08-2005
		KR	20050012243 A	31-01-2005
		RU	2315355 C2	20-01-2008
		US	2005225077 A1	13-10-2005
WO	03096268 A1	20-11-2003		

WO 2009126999 A1	22-10-2009	AU	2009238209 A1	22-10-2009
		CN	102057533 A	11-05-2011
		EP	2286485 A1	23-02-2011
		NZ	589319 A	25-05-2012
		PL	2286485 T3	28-02-2017
		WO	2009126999 A1	22-10-2009
