

①⑨ RÉPUBLIQUE FRANÇAISE  
INSTITUT NATIONAL  
DE LA PROPRIÉTÉ INDUSTRIELLE  
PARIS

①① N° de publication :

2 964 778

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

②① N° d'enregistrement national :

10 57383

⑤① Int Cl<sup>8</sup> : G 08 C 19/10 (2006.01)

⑫

DEMANDE DE BREVET D'INVENTION

A1

②② Date de dépôt : 15.09.10.

③③ Priorité :

④③ Date de mise à la disposition du public de la  
demande : 16.03.12 Bulletin 12/11.

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

⑥⑥ Références à d'autres documents nationaux  
apparentés :

⑦① Demandeur(s) : COMPAGNIE INDUSTRIELLE ET  
FINANCIERE D'INGENIERIE "INGENICO" Société  
anonyme — FR.

⑦② Inventeur(s) : ROSSI LAURENT et SCHANG BER-  
NARD.

⑦③ Titulaire(s) : COMPAGNIE INDUSTRIELLE ET  
FINANCIERE D'INGENIERIE "INGENICO" Société  
anonyme.

⑦④ Mandataire(s) : CABINET PATRICE VIDON.

⑤④ DISPOSITIF DE PROTECTION D'UN CONNECTEUR ET D'UN FIL DE COMMUNICATION D'UN LECTEUR DE  
CARTE A MEMOIRE.

⑤⑦ L'invention concerne un dispositif de protection d'un  
terminal de paiement électronique, comprenant un circuit  
imprimé électronique et un boîtier.

Selon l'invention, ledit dispositif comprend :

- dans un volume formé par un premier plan de masse  
dudit circuit imprimé et un second plan de masse disposé  
sur une surface interne dudit boîtier, un détecteur capacitif  
configuré pour délivrer une capacité de référence;
- un microprocesseur de mesure capacitive détectant  
une variation de capacité dudit détecteur;
- des moyens de transmission de ladite variation, lors-  
qu'une valeur absolue d'une différence entre lesdites capa-  
cités de référence et mesurée, excède un seuil  
prédéterminé.

FR 2 964 778 - A1



## **Dispositif de protection d'un connecteur et d'un fil de communication d'un lecteur de carte à mémoire.**

### **1 DOMAINE DE L'INVENTION**

La présente invention se rapporte au domaine de la protection des lecteurs  
5 de carte à mémoire comprenant un connecteur de carte à mémoire (CAM). Des  
lecteurs de carte à mémoire sont notamment employés dans de nombreux  
appareils tels que des terminaux de paiement, des dispositifs d'authentification ou  
d'identification ou encore des dispositifs de lecture de contenus.

La présente invention se rapporte plus particulièrement à la sécurisation  
10 d'un connecteur et d'une liaison de communication de tels lecteurs de carte à  
mémoire, afin de les protéger contre toutes intrusions de tiers malintentionnés.

### **2 ART ANTERIEUR**

Les appareils qui intègrent des lecteurs de carte à mémoire, tels que les  
terminaux de paiement électroniques (TPE) et les distributeurs automatiques de  
15 billets (DAB) constituent une pièce maîtresse du dispositif de sécurisation des  
paiements électroniques réalisés par les utilisateurs.

En effet, les terminaux de paiement électroniques permettent de faire le  
lien entre la carte de paiement et son porteur, entre le fournisseur et le réseau. En  
outre, ils enregistrent la transaction.

20 Les distributeurs automatiques de billets permettent le retrait de billets de  
banque après identification du porteur. Ils sont systématiquement connectés au  
centre informatique des banques émettrices de carte lors de chaque transaction.  
Les établissements de crédit sont responsables de leur fonctionnement.

Ces terminaux de paiement, comprennent de nombreux dispositifs de  
25 sécurisation et mettent en œuvre de nombreuses méthodes permettant d'assurer  
que les appareils sont utilisés conformément aux usages pour lesquels ils ont été  
prévus et respectent des normes de sécurité qui sont imposés par des organismes  
de certification.

Par exemple, dans le domaine des terminaux de paiement électroniques (TPE) les fabricants sont contraints de respecter depuis de 1er Janvier 2008, la norme PCI PED 2.0 (Payment Card Industry Pin Entry Device).

5 Cette norme sécuritaire consiste notamment à sécuriser le clavier de saisie des terminaux en protégeant la saisie du code confidentiel, et à bloquer le terminal en cas d'intrusion (frauduleuse ou accidentelle).

Cependant, outre la sécurisation du clavier, l'expérience montre que la mise à disposition de terminaux de paiement sur des points de vente permet aux tiers malintentionnés un accès relativement aisé à ces terminaux de paiement. Une  
10 des fraudes dernièrement constatée correspond au fait d'espionner les données confidentielles sur la liaison de communication d'entrée/sortie couramment désigné par l'acronyme « IO\_CAM », issu de l'anglais « *Input/Output* », l'acronyme CAM correspondant à l'expression « *carte à mémoire* ». Par ailleurs, on appelle Entrées-Sorties les échanges d'informations entre le processeur du  
15 terminal de paiement et les périphériques qui lui sont associés. Cette liaison de communication d'entrée/sorties est directement connectée au connecteur de carte à mémoire du terminal de paiement.

En janvier 2010, Ross Anderson, professeur de Cambridge, spécialiste de la sécurité informatique, a défrayé la chronique relative à la sécurisation des  
20 données. En effet, il a découvert comment fausser le dialogue entre une carte et un terminal de paiement, de manière à faire croire à tort à celui-ci que le porteur de cartes a tapé son code.

Ainsi, une nouvelle fraude correspond à l'introduction dans le terminal de paiement d'un leurre faisant croire au terminal de paiement que le porteur de carte  
25 bancaire a bel et bien tapé son code confidentiel. Une telle fraude correspond concrètement à l'insertion d'un micro « bug » ou anomalie logicielle dans la fente d'insertion du connecteur de carte de paiement.

Un tel « bug » peut prendre des formes diverses, par exemple le « bug » peut être un micro montage électronique servant à espionner les données  
30 transactionnelles entre la carte de paiement et le terminal de paiement. Le « bug »

peut également correspondre à une simple liaison insérée dans le connecteur de carte à mémoire, reliant la liaison de communication d'entrée/sorties du terminal de paiement à un montage externe destiné, à espionner, ou à tout autre action malveillante à l'encontre des données bancaires d'un utilisateur.

5            Afin de protéger la liaison d'entrées/sorties et le connecteur de carte à mémoire, des solutions de protection ont été développées. Ces solutions sont de type « electro-mécanique », mettant par exemple en œuvre un grillage flexible (en anglais, « *wire mesh* ») ou encore un treillis de liaisons sur lequel des tests de tensions sont par exemple effectués.

10           Ces solutions coûteuses visent explicitement à empêcher l'accès par un tiers malintentionné aux liaisons d'entrées/sorties et au connecteur de carte à mémoire.

De façon générale on associe en parallèle plusieurs « Wire mesh » ou treillis de liaisons pour protéger la liaison d'entrées/sorties « IO\_CAM ». Un  
15 treillis de liaisons implanté dans une des couches internes du PCB (circuit électronique imprimé) peut être utilisé pour protéger le côté inférieur du connecteur « CAM », tandis qu'un « wire mesh » (flexible possédant des pistes adjacentes couvrant la superficie à protéger) sera disposé côté supérieur du connecteur, un troisième dispositif (cache IO) pourra être déployé juste en face  
20 des broches de connections reliant le connecteur au PCB. Ce dernier dispositif est un mini circuit imprimé dans lequel est implanté un treillis de liaisons, le tout étant connecté (soudé) au circuit imprimé principal de façon à réaliser un « mini mur » entre les broches de connections et la fente d'insertion du connecteur.

Ces divers dispositifs sont testés sur des niveaux de tensions ou signaux.

25           L'inconvénient de ces solutions réside dans le fait que le grillage par nature possède des orifices qui rendent possible une éventuelle intrusion dans le connecteur de carte à mémoire ou encore une éventuelle dégradation de la liaison d'entrées/sorties.

Ainsi, à ce jour, les inventeurs n'ont identifié aucune solution simple et  
30 peu coûteuse permettant une protection mais également une surveillance efficace

de la liaison d'entrées/sorties et du connecteur de carte à mémoire contre toutes intrusions de tiers malintentionnés.

### 3 RESUME DE L'INVENTION

L'invention ne présente pas ces inconvénients de l'art antérieur. En effet  
5 l'invention concerne un dispositif de protection d'un terminal de paiement électronique, comprenant un circuit imprimé électronique et un boîtier.

Selon l'invention, un tel dispositif de protection comprend :

- au moins un détecteur capacitif disposé dans un volume formé par un premier plan de masse dudit circuit imprimé et un second plan de masse  
10 disposé sur une surface interne dudit boîtier, ledit au moins un détecteur capacitif étant configuré pour délivrer une capacité de référence ;
- un microprocesseur de mesure capacitive relié électriquement audit au moins un détecteur capacitif, ledit au moins un microprocesseur étant configuré pour détecter une variation de capacité dudit au moins un  
15 détecteur capacitif ;
- des moyens de transmission d'une information représentative de ladite variation de capacité, lorsqu'une valeur absolue d'une différence entre ladite capacité mesurée et ladite capacité de référence excède un seuil prédéterminé.

20 Selon une caractéristique particulière de l'invention, ledit dispositif de protection utilise un détecteur (wire mesh) existant et réalise une mesure de capacité sur ledit détecteur.

Selon un mode de réalisation particulier, ledit dispositif de protection comprend en outre des moyens de calibrage délivrant ladite capacité de référence.

25 Selon un mode de réalisation particulier ledit dispositif de protection comprend en outre un système de compensation environnemental modifiant ladite capacité de référence en fonction d'un critère prédéterminé.

Selon une caractéristique particulière, ledit au moins un détecteur capacitif est disposé sur appelé premier détecteur capacitif est disposé sur un connecteur de  
30 carte à mémoire.

Selon une caractéristique particulière, ledit dispositif de protection comprend en outre un deuxième détecteur capacitif connecté à une liaison entrée/sortie du connecteur de carte à mémoire.

5 Selon un mode de réalisation particulier, ledit premier détecteur capacitif est une piste de cuivre de forme spirale carrée.

Selon un mode de réalisation particulier, ledit premier détecteur capacitif est déployé selon un plan plein.

10 Selon un autre aspect, l'invention concerne également un procédé de protection d'un terminal de paiement électronique, comprenant un circuit imprimé électronique et un boîtier. Selon l'invention, un tel procédé de protection comprend :

- une étape de disposition d'au moins un détecteur capacitif dans un volume formé par un premier plan de masse dudit circuit imprimé et un second plan de masse disposé sur une surface interne dudit boîtier, ledit au moins un détecteur capacitif étant configuré pour délivrer une capacité de référence ;
- une étape de mesure capacitive mise en œuvre par un microprocesseur de mesure capacitive relié électriquement audit au moins un détecteur capacitif, ledit au moins un microprocesseur étant configuré pour détecter
- 20 une variation de capacité dudit au moins un détecteur capacitif ;
- une étape de transmission d'une information représentative de ladite variation de capacité, lorsqu'une valeur absolue d'une différence entre ladite capacité mesurée et ladite capacité de référence excède un seuil prédéterminé.

25 Selon une caractéristique particulière, ledit procédé de protection comprend en outre une étape de calibrage délivrant ladite capacité de référence.

Selon un autre aspect, l'invention se rapporte également à un terminal de paiement. Selon l'invention, un tel terminal de paiement comprend un dispositif de protection tel que décrit préalablement.

Selon un autre aspect, l'invention concerne également un programme d'ordinateur qui comprend des instructions de code programme pour la mise en œuvre du procédé de protection lorsque le programme est exécuté par un processeur.

#### 5 4 LISTE DES FIGURES

D'autres caractéristiques et avantages de l'invention apparaîtront plus clairement à la lecture de la description suivante d'un mode de réalisation préférentiel, donné à titre de simple exemple illustratif et non limitatif, et des dessins annexés, parmi lesquels :

- 10 - la figure 1 illustre un schéma d'un dispositif de protection selon l'invention ;
- la figure 2 illustre des courbes de calibrage du dispositif de protection selon l'invention ;
- les figures 3A à 3D, présentent la disposition et le fonctionnement d'un  
15 détecteur capacitif sur un connecteur de carte mémoire, ainsi que deux variantes de détecteur capacitif ;
- les figures 4A et 4B, présentent respectivement le schéma d'un deuxième mode de réalisation de l'invention, et la structure électronique du deuxième détecteur capacitif associé ;
- 20 - la figure 5 illustre le procédé de protection selon l'invention ;
- La figure 6 schématise un terminal de paiement selon l'invention.

#### 5 DESCRIPTION DETAILLEE DE L'INVENTION

##### 5.1 Rappel du principe de l'invention

L'invention propose de surveiller efficacement et simplement la liaison  
25 d'entrées/sorties et du connecteur de carte à mémoire contre toutes intrusions de tiers malintentionnés, en utilisant un dispositif de protection mettant en œuvre une mesure capacitive d'au moins un détecteur capacitif disposé sur le connecteur de carte à mémoire d'un terminal de paiement.

Comme le dispositif de protection met en œuvre une mesure capacitive,  
30 une intrusion d'un élément conducteur est détectée du fait que l'intrusion modifie

les lignes de champs magnétiques, et par voie de conséquence la capacité de référence du détecteur capacitif au-delà d'un seuil prédéterminé.

Selon l'invention, le dispositif de protection d'un terminal de paiement comprend au moins un détecteur capacitif introduit dans un volume formé par un premier plan de masse reposant sur la surface du circuit imprimé du terminal de paiement et un second plan de masse disposé au fond du boîtier plastique du terminal de paiement, un microprocesseur de mesure capacitive et des moyens de transmission d'une information signalant une variation de la capacité du détecteur capacitif au-delà d'un seuil prédéterminé, signalant en d'autres termes une intrusion dans le volume surveillé.

Selon un premier mode de réalisation de l'invention, un premier détecteur capacitif est déployé sur un connecteur de carte à mémoire du terminal de paiement.

Selon un autre mode de réalisation, un deuxième détecteur capacitif est ajouté dans le dispositif de protection et relié à une liaison d'entrée/sortie du connecteur de carte à mémoire.

Selon l'invention, le dispositif de protection est apte à protéger par mesure capacitive un terminal de paiement. Un tel dispositif de protection peut se présenter sous n'importe quelle forme. La forme du dispositif peut être adaptée en fonction du boîtier, ou encore du connecteur de carte à mémoire à protéger.

Par la suite, on détaille un mode de réalisation d'un dispositif de protection selon l'invention. Il est clair cependant que l'invention ne se limite pas à cette application particulière, mais peut également être mise en œuvre dans de nombreux autres contextes de protection de circuits imprimés électroniques et plus généralement dans tous les cas où les caractéristiques listées par la suite sont intéressantes.

#### Structure générale d'un dispositif selon l'invention

On présente en relation avec la figure 1, la structure générale d'un dispositif de protection 10 selon l'invention. Un tel dispositif comprend tout d'abord un détecteur capacitif 12 appartenant à un volume défini par un premier



plan de masse 111 d'un circuit imprimé électronique 11 et par un second plan de masse 112 disposé au fond du boîtier du terminal de paiement.

Ces plans de masse produisent une action comparable à celle d'une cage de Faraday, c'est-à-dire qu'ils permettent de protéger le dispositif de protection d'éventuelles perturbations électromagnétiques extérieures.

Le plan de masse disposé sur le fond du boîtier du terminal de paiement est par exemple obtenu au moyen d'un procédé d'étalement de peinture conductrice connu.

Par ailleurs, des moyens de calibrage 15, reliés électriquement au détecteur capacitif, permettent d'en évaluer la capacité de référence. Ces moyens de calibrage 15 seront par la suite davantage détaillés.

En outre, le dispositif de protection selon l'invention comprend également un microprocesseur de mesure capacitive 13 relié électriquement au détecteur capacitif 12 et à la masse 16. Un tel microprocesseur de mesure utilise par exemple un capteur capacitif correspondant à une sonde pour mesurer la capacité du détecteur capacitif.

Une telle sonde est très généralement réalisée avec une électrode plane de mesure entourée d'un anneau de garde. L'électrode forme alors avec le détecteur capacitif un condensateur plan. Une électrode de garde contenue dans l'anneau de garde est placée autour de celle de mesure et son potentiel est porté à la même valeur afin d'améliorer la linéarité en rendant les lignes de champ normales (perpendiculaires) à l'électrode de mesure. L'électrode de garde permet ainsi d'éliminer les effets de bord.

Grâce à ces moyens de mesure 13, une variation de la capacité du détecteur capacitif est détectée. Cette variation est par exemple obtenue en comparant la capacité mesurée à la capacité de référence préalablement déterminée par les moyens de calibrage 15. Cette mesure est préférentiellement effectuée en temps réel afin d'avertir instantanément le processeur sécurisé d'un terminal de paiement via des moyens de transmission 14.

Indépendamment de la fréquence de mesure sélectionnée par l'utilisateur, l'ensemble des mesures est piloté par un programme d'ordinateur enregistré au sein des moyens de mesures.

Plus précisément, les moyens de mesure déterminent une différence entre  
5 la capacité du détecteur capacitif mesurée par les moyens de mesure 13, et la capacité de référence déterminée par les moyens de calibrage. Si la valeur absolue de cette différence excède un seuil prédéterminé  $S$ , les moyens de transmission du dispositif de protection selon l'invention signalent au processeur sécurisé du terminal sécurisé de se mettre en mode « *attaque* ».

10 Ainsi, le dispositif de protection selon l'invention permet de déterminer tout contact avec le détecteur capacitif disposé dans un volume défini par le premier plan de masse 111 du circuit imprimé électronique 11 et par le second plan de masse 112 disposé au fond du boîtier du terminal de paiement à protéger. En particulier, toute intrusion (même sans contact direct avec le capteur) par un  
15 tiers malintentionné sera détectée, du fait que cette intrusion, notamment par l'introduction d'un élément conducteur modifie de façon significative la capacité du détecteur capacitif.

En outre, ce dispositif de protection tire profit du détecteur capacitif et de la mesure capacitive en évitant de mettre en œuvre un routage géométrique  
20 complexe ou encore en évitant d'utiliser un matériel de protection facilement dégradable et onéreux tel que des grillages flexibles.

#### Moyens de calibrage du détecteur capacitif considéré

Le calibrage mis en œuvre par les moyens de calibrage 15, est nécessaire du fait que la valeur de la capacité est sensible aux variations extérieures.

25 En effet, il est connu que la valeur de capacité varie en fonction de différents facteurs. Par exemple, la capacité d'un détecteur capacitif varie en fonction de l'hystérésis de charge dû à la magnétisation d'un matériau, l'effet d'une batterie du terminal de paiement, ou encore la température, l'humidité, le vieillissement notamment par oxydation des matériaux constituant le détecteur  
30 capacitif, etc.

On présente en relation avec la figure 2, représentant un exemple de courbes de calibrage du dispositif de protection selon l'invention, la procédure mise en œuvre par les moyens de calibrage délivrant la capacité de référence du détecteur capacitif.

5 Les moyens de calibrage mesurent 21 (par exemple d'une manière similaire à celle utilisée par les moyens de mesure précédemment décrits) la capacité du détecteur capacitif en fonction du temps. La courbe de mesure 21 représentée sur la figure 2 atteste que la capacité varie en fonction du temps, notamment en fonction de la température environnante.

10 Les moyens de calibrage moyennent les données de mesure de capacité de la courbe de mesure de sorte qu'une valeur de référence *Ref* est obtenue.

En outre, les moyens de calibrage déterminent par exemple un seuil de variation *S* de capacité au-delà duquel la variation de capacité est anormale. Ainsi, les moyens de calibrage déterminent la plage de valeur de capacités centrée sur la  
15 valeur de référence permettant d'attester un fonctionnement « *normal* » et sécurisé du circuit imprimé du terminal de paiement.

Préférentiellement, la valeur de référence et le seuil prédéterminé *S* sont enregistrés dans une mémoire et transmis aux moyens de mesure afin que ces derniers déterminent une intrusion d'un tiers malintentionné visant à détériorer le  
20 circuit imprimé électronique.

De manière optionnelle, les moyens de calibrages comprennent en outre un système de compensation environnemental visant à adapter les valeurs de référence et de seuil prédéterminé *S* en fonction d'un paramètre sélectionné par l'utilisateur du terminal de paiement.

25 Par exemple, la température ambiante à Singapour étant très différente de la température à Stockholm, l'utilisateur adapte en fonction de sa localisation la référence et la plage de variation de capacité autorisée.

De même selon un autre exemple, l'utilisateur peut adapter cette plage de variation au fur et à mesure du vieillissement du terminal de paiement, selon des  
30 recommandations du constructeur mentionnées dans une notice d'utilisation.

## 5.2 Description d'un premier mode de réalisation d'un dispositif selon l'invention

### Structure du dispositif de protection selon ce premier mode de réalisation

On présente dans ce mode de réalisation représenté par les figures 3A à 3D, un dispositif de protection selon l'invention dans lequel un premier détecteur capacitif a été monté sur le connecteur de carte à mémoire représenté sur la figure 3A.

Le premier détecteur capacitif placé sur le connecteur de carte à mémoire mesure dans un volume défini par un premier plan de masse 111 d'un circuit imprimé électronique 11 et par un second plan de masse 112 disposé au fond du boîtier du terminal de paiement, la capacité de ce volume.

Ainsi, toute introduction d'un objet même très petit, constitué d'une ou plusieurs parties conductrices, entre le détecteur capacitif et l'un des plans de masse (définissant le volume contenant le détecteur capacitif), modifie les lignes de champs 32 représentées sur la figure 3B.

Cette modification de lignes de champs entraîne une variation de la capacité du volume au delà du seuil prédéterminé défini précédemment par les moyens de calibrage.

### Type de détecteur capacitif

Un détecteur capacitif prenant la forme d'une simple piste de cuivre est par exemple utilisé et représenté sur la figure 3C. Cette piste prend par exemple la forme d'une spirale carrée 33.

Selon une autre variante, le détecteur 12 correspond à un plan plein 34 et est disposé sur une surface du connecteur à carte mémoire du terminal de paiement par exemple.

Un détecteur capacitif correspondant à un plan plein, prend la forme d'une surface capacitive. Plus précisément, une technologie capacitive de surface consiste en un revêtement conducteur uniforme sur un isolant. Lors de l'utilisation, des électrodes placées sur le bord de l'isolant répartissent un courant de faible tension de manière égale sur toute la couche conductrice, créant ainsi un

champ électrique uniforme. Lorsqu'un objet rentre en contact avec la surface, cela a pour effet d'attirer le courant de chaque coin du champ électrique.

De manière optionnelle, un contrôleur calcule les coordonnées du contact en mesurant le courant. Il transmet ensuite ces coordonnées au processeur sécurisé  
5 du terminal de paiement.

Selon un autre mode de réalisation, le détecteur capacitif peut prendre la forme d'un treillis (non représenté) de fils conducteurs très fins (moins de 10  $\mu\text{m}$ ) noyé entre des couches d'isolant pare exemple du verre ou des films de plastique laminés.

10 Un tel treillis peut être plan ou tridimensionnel avec un maillage plus ou moins dense. Un simple fil, qui est disposé de façon particulière, peut également être suffisant dans certains cas de figure.

Par ailleurs, le dispositif de protection selon l'invention peut également être connecté électriquement à un circuit imprimé possédant un détecteur capacitif  
15 existant constitué d'une partie conductrice et d'une partie isolante. Dans ce cas, le dispositif de protection selon l'invention place des électrodes sur le bord de l'isolant afin de répartir un courant de faible tension de manière égale sur toute la partie conductrice, créant ainsi un champ électrique uniforme. Le détecteur existant est par ce biais rendu capacitif.

### 20 5.3 Description d'un deuxième mode de réalisation d'un dispositif selon l'invention

On représente en relation avec la figure 4A, le schéma d'un deuxième mode de réalisation de l'invention. Ce deuxième mode de réalisation ajoute en plus du premier détecteur capacitif 41 disposé sur le connecteur de carte à  
25 mémoire, un deuxième détecteur capacitif afin d'interdire l'accès aux liaisons du connecteur de carte à mémoire, en particulier la liaison « IO\_CAM » (de l'anglais pour « Input/output »).

Comme illustré en figure 4A, le connecteur de carte à mémoire 42 est monté sur le circuit imprimé 43. Le connecteur de carte à mémoire présente une  
30 fente 42.1 dans laquelle la carte peut être introduite. Le connecteur de carte à

mémoire comprend également un ensemble de liaisons 42.2 permettant une connexion de la carte, une fois que celle-ci est insérée, avec un processeur de l'appareil.

Ces liaisons 42.2 présentent un léger renflement 42.3 au niveau de la zone de connexion avec la carte, au sein du connecteur de carte à mémoire. Les liaisons sont ensuite conformées pour qu'elles s'étendent vers le circuit imprimé 43. Elles rejoignent celui-ci au niveau d'une zone intermédiaire dans laquelle les liaisons 42.4 sont reliées au circuit imprimé 43.

Le deuxième détecteur capacitif 44 est disposé de sorte qu'il empêche l'accès à au moins certaines liaisons et notamment la liaison « IO\_CAM ».

Une structure électronique du deuxième détecteur capacitif est représentée en relation avec la figure 4B. Selon cette structure, un condensateur de liaison *CL* met en œuvre un couplage capacitif permettant d'évaluer la capacité de la liaison IO\_CAM. Par ailleurs, ce détecteur est alimenté par une tension nominale *Vcam* et comprend en outre une résistance *R* et une capacité parasite *CP*.

*Vcam* et *R* dépendent du terminal et plus particulièrement des normes EMV et sont présentés dans tous les terminaux de paiement. La capacité de liaison *CL* est directement liée à l'invention, elle est d'une valeur de 220 pF (à titre indicatif), cette valeur peut varier en fonction des dimensions des pistes.

#### 5.4 Description d'un mode de réalisation du procédé de protection selon l'invention

On présente en relation avec la figure 5, le procédé de protection 50 d'un circuit imprimé électronique selon l'invention.

Un tel procédé comprend

- une étape de disposition 51 d'au moins un détecteur capacitif sur une couche du circuit imprimé du terminal de paiement,
- une étape de calibrage 52 délivrant la capacité de référence du détecteur capacitif,
- une étape de mesure capacitive 53 mise en œuvre par un microprocesseur de mesure capacitive relié électriquement au

- détecteur capacitif, le microprocesseur étant configuré pour détecter une variation de capacité du détecteur capacitif ;
- une étape de transmission 54 d'une information représentative « *Attaque !* » de la variation de capacité, lorsqu'une valeur absolue d'une différence entre la capacité mesurée et la capacité de référence excède un seuil prédéterminé.

En outre, l'étape de calibrage pourra être réitérée selon une procédure d'utilisation connue de l'utilisateur.

Selon un mode de réalisation particulier, l'étape de calibrage comprend en outre une étape de compensation environnementale, visant à prendre en compte l'influence naturelle de certains paramètres tels que : l'hystérésis de charge dû à la magnétisation d'un matériau, l'effet d'une batterie du terminal de paiement, ou encore la température, l'humidité, le vieillissement notamment par oxydation des matériaux constituant le détecteur capacitif, etc.

Le procédé de protection mise en œuvre par un dispositif de protection conforme au deuxième mode de réalisation décrit précédemment, met en œuvre deux détecteurs capacitifs, l'un étant disposé sur le connecteur de carte à mémoire et l'autre relié à la liaison d'entrée/sortie du connecteur de carte à mémoire. Les étapes du procédé précédemment décrit sont en conséquence effectuées pour chaque détecteur capacitif mis en œuvre.

On présente, en relation avec la figure 6, un mode de réalisation d'un terminal de paiement selon l'invention.

Un tel terminal comprend une mémoire 61 constituée d'une mémoire tampon, une unité de traitement 62, équipée par exemple d'un microprocesseur P, et pilotée par le programme d'ordinateur 63, mettant en œuvre le procédé de protection selon l'invention.

A l'initialisation, les instructions de code du programme d'ordinateur 63 sont par exemple chargées dans une mémoire RAM avant d'être exécutées par le processeur de l'unité de traitement 62. L'unité de traitement 62 reçoit en entrée au moins une information I, telle que des identifiants de zones de localisation. Le

microprocesseur de l'unité de traitement 62 met en œuvre les étapes du procédé de protection décrit précédemment, selon les instructions du programme d'ordinateur 63, pour délivrer une information traitée T, telle que la détection d'une attaque entraînant la suppression des données protégées. Pour cela, le

5 terminal comprend, outre la mémoire tampon 61, au moins un détecteur capacitif disposé dans un volume formé par un premier plan de masse dudit circuit imprimé et un second plan de masse disposé sur une surface interne dudit boîtier, ledit au moins un détecteur capacitif étant configuré pour délivrer une capacité de référence, un microprocesseur de mesure capacitive relié électriquement audit au

10 moins un détecteur capacitif, ledit au moins un microprocesseur étant configuré pour détecter une variation de capacité dudit au moins un détecteur capacitif, des moyens de transmission d'une information représentative de ladite variation de capacité, lorsqu'une valeur absolue d'une différence entre ladite capacité mesurée et ladite capacité de référence excède un seuil prédéterminé.

15 Ces moyens sont pilotés par le microprocesseur de l'unité de traitement 62.



## REVENDICATIONS

1. Dispositif de protection d'un terminal de paiement électronique, comprenant un circuit imprimé électronique et un boîtier, caractérisé en ce  
5 que ledit dispositif de protection comprend :
  - au moins un détecteur capacitif disposé dans un volume formé par un premier plan de masse dudit circuit imprimé et un second plan de masse disposé sur une surface interne dudit boîtier, ledit au moins un détecteur capacitif étant configuré pour délivrer une  
10 capacité de référence ;
  - un microprocesseur de mesure capacitive relié électriquement audit au moins un détecteur capacitif, ledit au moins un microprocesseur étant configuré pour détecter une variation de capacité dudit au moins un détecteur capacitif ;
  - 15 - des moyens de transmission d'une information représentative de ladite variation de capacité, lorsqu'une valeur absolue d'une différence entre ladite capacité mesurée et ladite capacité de référence excède un seuil prédéterminé.
2. Dispositif de protection selon la revendication 1, caractérisé en ce qu'il  
20 comprend en outre des moyens de calibrage délivrant ladite capacité de référence.
3. Dispositif de protection selon la revendication 1, caractérisé en ce que ledit au moins un détecteur capacitif est disposé sur appelé premier détecteur capacitif est disposé sur un connecteur de carte à mémoire.
- 25 4. Dispositif de protection selon la revendication 1, caractérisé en ce qu'il comprend en outre un deuxième détecteur capacitif connecté à une liaison entrée/sortie du connecteur de carte à mémoire.
5. Dispositif de protection selon la revendication 1, caractérisé en ce que ledit premier détecteur capacitif est une piste de cuivre de forme spirale carrée.
- 30 6. Dispositif de protection selon la revendication 1, caractérisé en ce que ledit

premier détecteur capacitif est déployé selon un plan plein.

7. Procédé de protection d'un terminal de paiement électronique, comprenant un circuit imprimé électronique et un boîtier, caractérisé en ce que ledit procédé de protection comprend :
  - 5 - une étape de disposition d'au moins un détecteur capacitif dans un volume formé par un premier plan de masse dudit circuit imprimé et un second plan de masse disposé sur une surface interne dudit boîtier, ledit au moins un détecteur capacitif étant configuré pour délivrer une capacité de référence ;
  - 10 - une étape de mesure capacitive mise en œuvre par un microprocesseur de mesure capacitive relié électriquement audit au moins un détecteur capacitif, ledit au moins un microprocesseur étant configuré pour détecter une variation de capacité dudit au moins un détecteur capacitif ;
  - 15 - une étape de transmission d'une information représentative de ladite variation de capacité, lorsqu'une valeur absolue d'une différence entre ladite capacité mesurée et ladite capacité de référence excède un seuil prédéterminé.
8. Procédé de protection selon la revendication 7, caractérisé en ce qu'il comprend en outre une étape de calibrage délivrant ladite capacité de référence.
9. Terminal de paiement, caractérisé en ce qu'il comprend un dispositif de protection selon la revendication 1.
10. Programme d'ordinateur caractérisé en ce qu'il comprend des instructions de code programme pour la mise en œuvre du procédé de protection selon la revendication 7, lorsque le programme est exécuté par un processeur.

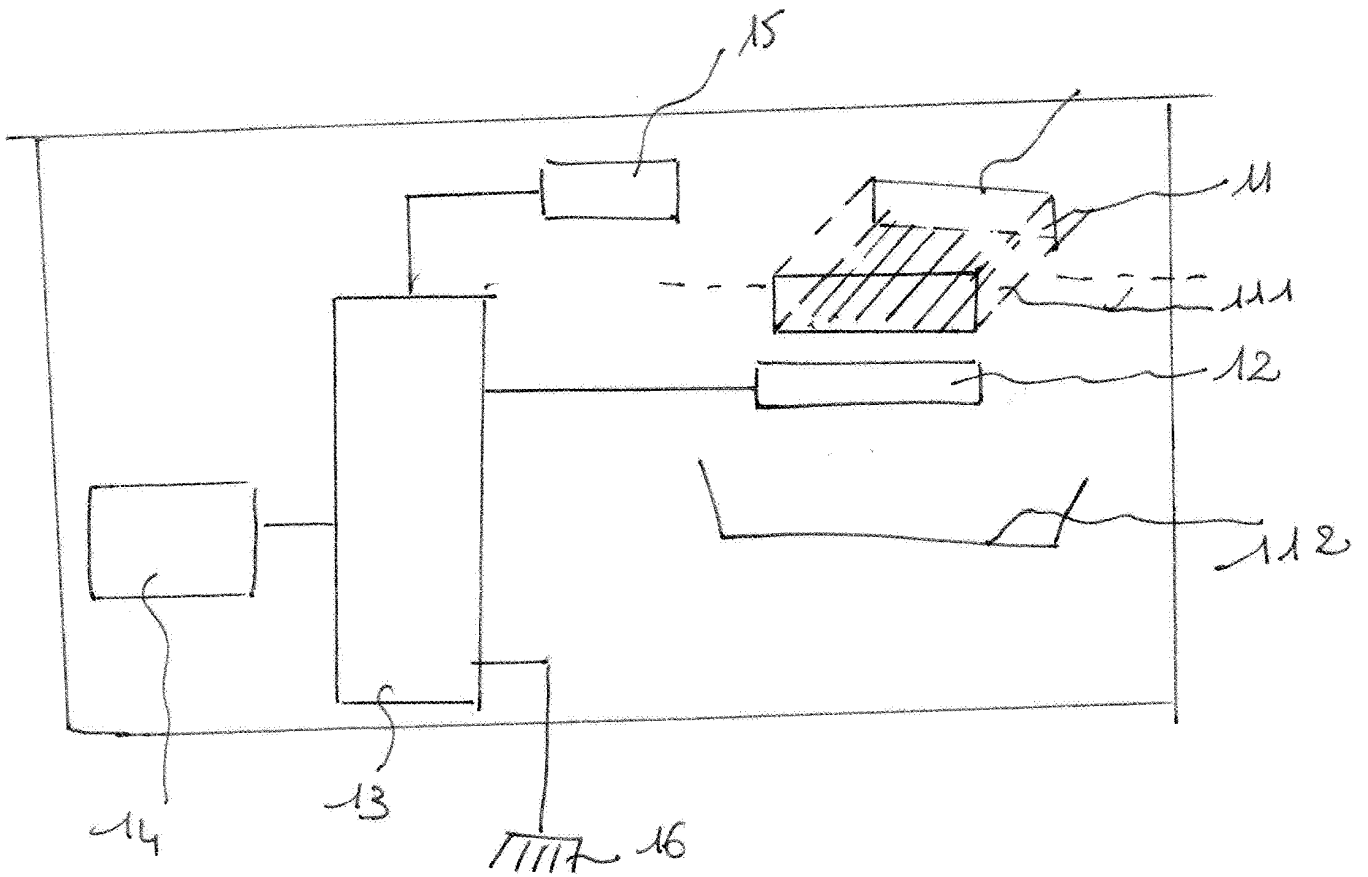


Figure 1

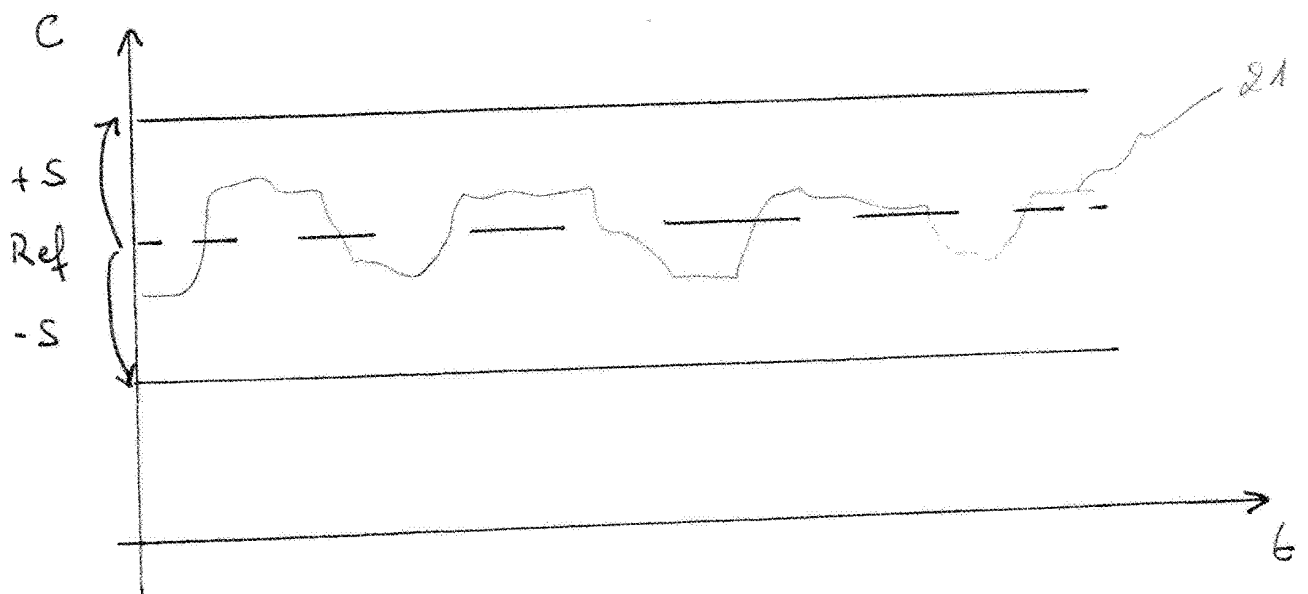


Figure 2

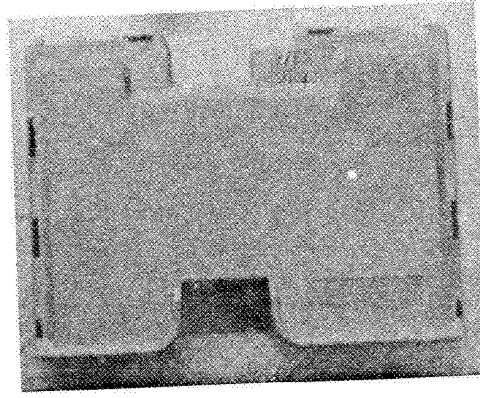


Figure 3A

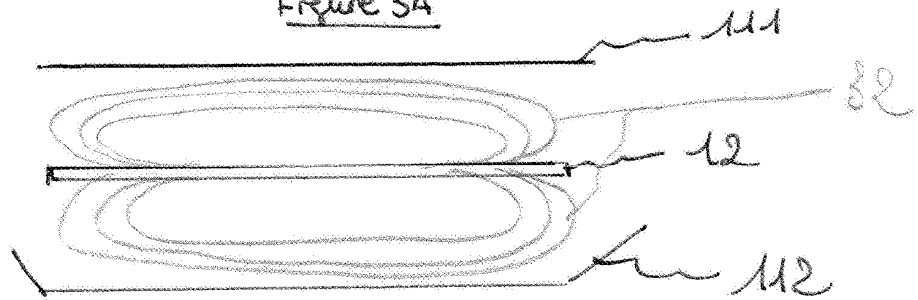


Figure 3B

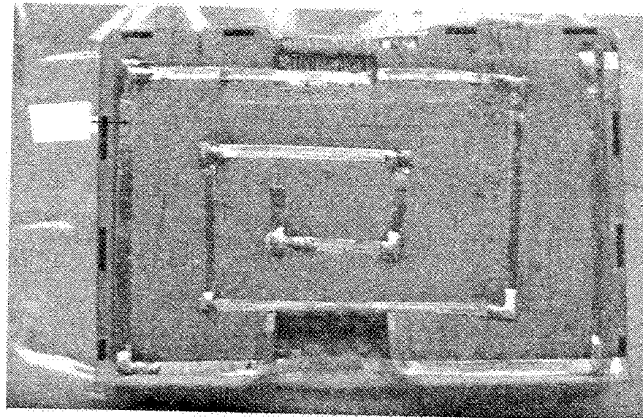


Figure 3C

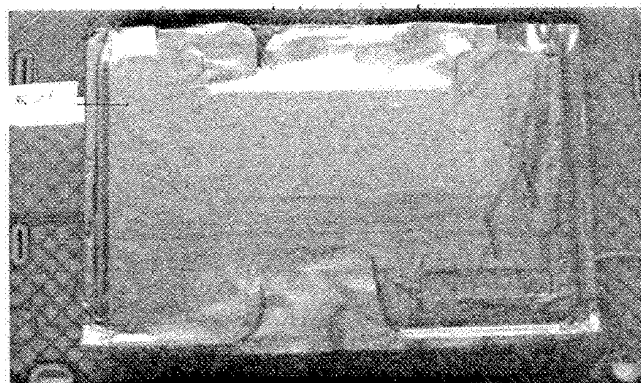


Figure 3D

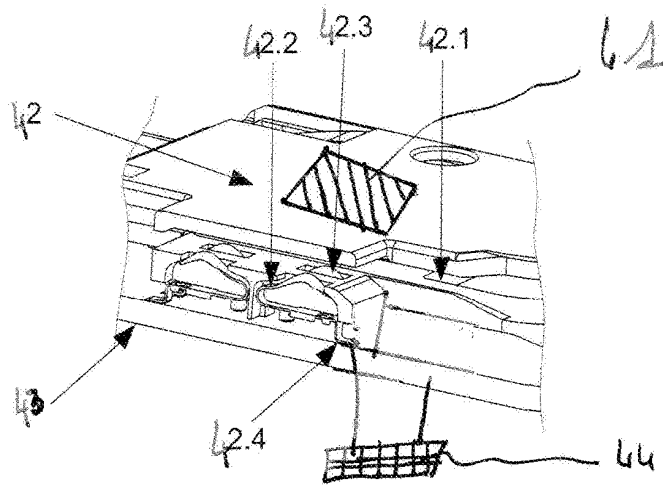


Figure 4A

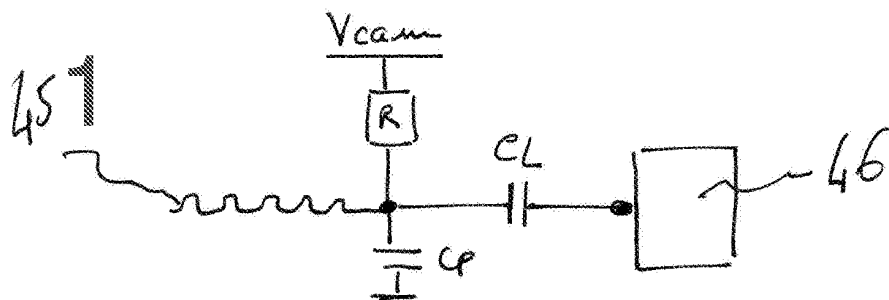


Figure 4B

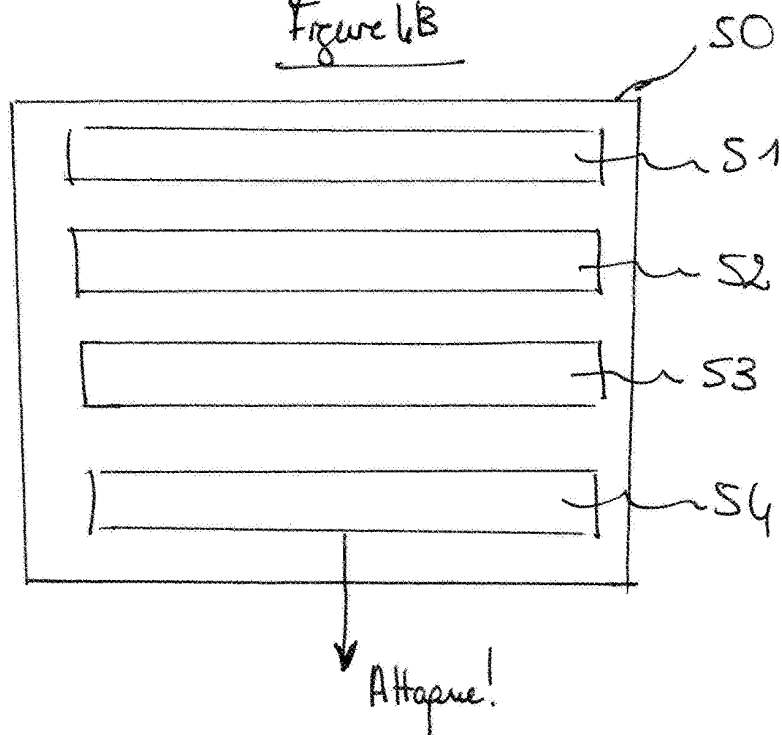
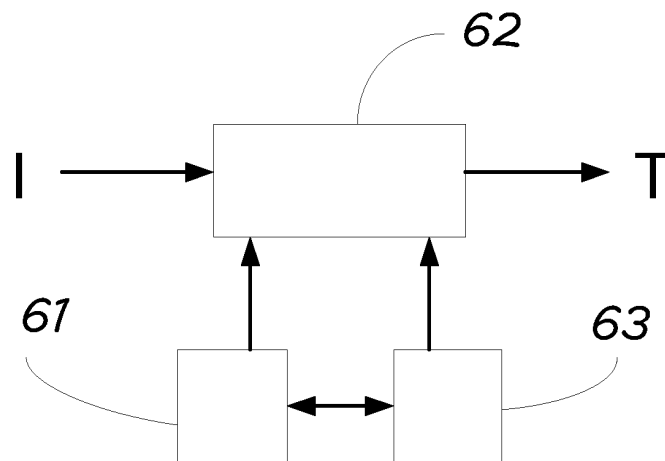


Figure 5



*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 748460  
FR 1057383

| DOCUMENTS CONSIDÉRÉS COMME PERTINENTS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                              | Revendication(s)<br>concernée(s) | Classement attribué<br>à l'invention par l'INPI |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|----------------------------------|-------------------------------------------------|
| Catégorie                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Citation du document avec indication, en cas de besoin,<br>des parties pertinentes           |                                  |                                                 |
| A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | EP 1 873 680 A1 (HOPT & SCHULER DDM [DE])<br>2 janvier 2008 (2008-01-02)<br>* figure 1 *     | 1,7                              | G08C19/10                                       |
| A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | EP 1 927 931 A1 (COACTIVE TECHNOLOGIES INC [US])<br>4 juin 2008 (2008-06-04)<br>* figure 1 * | 1,7                              |                                                 |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                              |                                  | DOMAINES TECHNIQUES<br>RECHERCHÉS (IPC)         |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                              |                                  | G06K<br>G07F                                    |
| Date d'achèvement de la recherche                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                              | Examineur                        |                                                 |
| 12 août 2011                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                              | de Ronde, Jan                    |                                                 |
| <p><b>CATÉGORIE DES DOCUMENTS CITÉS</b></p> <p>X : particulièrement pertinent à lui seul<br/>Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie<br/>A : arrière-plan technologique<br/>O : divulgation non-écrite<br/>P : document intercalaire</p> <p>T : théorie ou principe à la base de l'invention<br/>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.<br/>D : cité dans la demande<br/>L : cité pour d'autres raisons<br/>.....<br/>&amp; : membre de la même famille, document correspondant</p> |                                                                                              |                                  |                                                 |

**ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE**  
**RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1057383 FA 748460**

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 **12-08-2011**

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<br>au rapport de recherche |    | Date de<br>publication | Membre(s) de la<br>famille de brevet(s) | Date de<br>publication |
|-------------------------------------------------|----|------------------------|-----------------------------------------|------------------------|
| EP 1873680                                      | A1 | 02-01-2008             | CN 101093536 A                          | 26-12-2007             |
|                                                 |    |                        | US 2007295810 A1                        | 27-12-2007             |
| -----                                           |    |                        |                                         |                        |
| EP 1927931                                      | A1 | 04-06-2008             | AT 434230 T                             | 15-07-2009             |
|                                                 |    |                        | CN 101276976 A                          | 01-10-2008             |
|                                                 |    |                        | FR 2909469 A1                           | 06-06-2008             |
|                                                 |    |                        | US 2008132119 A1                        | 05-06-2008             |
| -----                                           |    |                        |                                         |                        |