

12

DEMANDE DE BREVET D'INVENTION

A1

22 Date de dépôt : 28.12.01.

30 Priorité :

43 Date de mise à la disposition du public de la
demande : 04.07.03 Bulletin 03/27.

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) : CENTRE D'ECHANGES DE DON-
NEES ET D'INFORMATION DU CREDIT AGRICOLE
MUTUEL CEDICAM — FR et COPERNIC CO LTD —
TH.

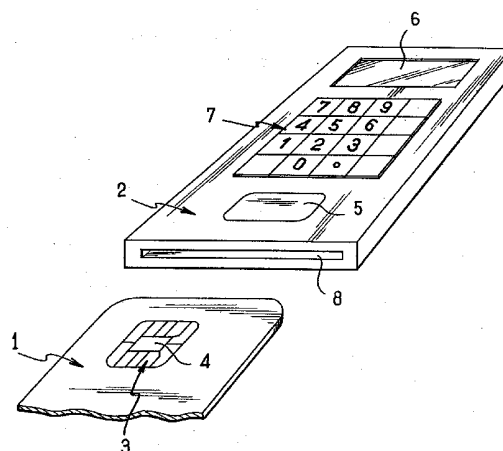
72 Inventeur(s) : CASSONE GIANNI.

73 Titulaire(s) :

74 Mandataire(s) : REGIMBEAU.

54 CARTE A PUCE AUTOVERROUILLABLE, DISPOSITIF DE SECURISATION D'UNE TELLE CARTE ET
PROCEDES ASSOCIES.

57 L'invention concerne un dispositif (2) de sécurisation
d'une carte à puce (1), caractérisé en ce qu'il comprend des
moyens d'évaluation de paramètres biologiques (5) d'un
porteur de la carte aptes à sélectivement autoriser la modi-
fication d'une valeur de compteur de la carte à puce pour un
nombre déterminé d'opérations autorisées, de manière à
déverrouiller ou à verrouiller la carte à puce.



L'invention concerne la sécurisation et l'utilisation de cartes à puce, notamment de cartes à puce bancaires.

5 Par exemple, dans le domaine bancaire, l'utilisation d'une carte à puce dite bancaire est actuellement assujettie à la validation de transaction par un code confidentiel composé de quatre chiffres. En cas d'utilisation frauduleuse par un tiers suite à une
10 perte ou à un vol, même en cas de compromission simultanée, par ruse ou par négligence, du code confidentiel de ladite carte, il n'existe pas de moyens d'invalider la carte avant d'avoir effectué un enregistrement de la déclaration de vol ou de perte de
15 ladite carte auprès d'un centre d'opposition. Cette déclaration ne pouvant pas être immédiate, il existe un intervalle de temps plus ou moins important durant lequel la carte bancaire peut enregistrer un grand nombre de transactions avant d'être invalidée. Ceci est
20 très préjudiciable pour le porteur de la carte.

Un but de l'invention est de fournir un dispositif apte à sécuriser une carte à puce de manière à la rendre inutilisable de manière simple et rapide.

25

Pour atteindre ce but, on prévoit selon l'invention, un dispositif de sécurisation d'une carte à puce, caractérisé en ce qu'il comprend des moyens d'évaluation de paramètres biologiques d'un porteur de
30 la carte aptes à sélectivement autoriser la modification d'une valeur de compteur de la carte à puce pour un nombre déterminé d'opérations autorisées, de manière à déverrouiller ou à verrouiller la carte à puce.

Un avantage essentiel est qu'une fois que le nombre d'opérations autorisées a été effectué, la carte à puce s'auto-verrouille et se retrouve inutilisable par la
5 suite, et ceci de manière simple et rapide.

Avantageusement, le dispositif de sécurisation peut présenter au moins l'une des caractéristiques optionnelles suivantes :

- 10 - les moyens d'évaluation de paramètres biologiques comprennent un capteur d'empreintes digitales,
- les moyens d'évaluation de paramètres biologiques comportent des premiers moyens de stockage aptes à mémoriser les paramètres biologiques du porteur,
- 15 - le dispositif comporte des deuxièmes moyens de stockage aptes à mémoriser une clé d'identification.

On prévoit aussi, selon l'invention, une carte,
20 notamment carte bancaire, comportant une puce électronique ainsi que des moyens d'interfaçage de la puce, caractérisée en ce que la puce comprend, dans une zone à accès contrôlé, une valeur de compteur de nombre d'opérations autorisées, capable d'être modifiée lors
25 d'une transmission d'informations par les moyens d'interfaçage, et des moyens de verrouillage aptes à verrouiller la carte lorsque la valeur de compteur atteint un seuil, la valeur de compteur pouvant être initialisée par une information spécifique transmise par
30 les moyens d'interfaçage.

Avantageusement, la carte peut présenter au moins l'une des caractéristiques optionnelles suivantes :

- lorsque la carte est du type associé à un code confidentiel, elle comprend des moyens aptes, lors de la réception dans la carte d'un code confidentiel erroné, à modifier la valeur de compteur, notamment à forcer
5 ladite valeur à la valeur du seuil.

- la carte comprend des moyens aptes, lors de la réception d'une information de validation d'une transaction effectuée, à modifier la valeur de compteur.

- la puce comporte des moyens de stockage d'une clé
10 d'identification.

- la clé d'identification est apte à autoriser le déverrouillage de la carte et/ou une initialisation de la valeur de compteur via les moyens d'interfaçage.

- les moyens d'interfaçage de la puce sont aptes à
15 coopérer avec un dispositif de sécurisation tel que défini plus haut.

On prévoit en outre, selon l'invention, un procédé de programmation pour un dispositif de sécurisation tel
20 que défini plus haut, caractérisé en ce qu'il comprend les étapes suivantes :

(A) insertion de la carte dans le dispositif de sécurisation,

(B) vérification de la correspondance entre une
25 information contenue dans le dispositif de mémorisation et une information contenue dans la puce de la carte,

(C) vérification des paramètres biologiques du porteur par les moyens d'évaluation de paramètres biologiques du dispositif de sécurisation,

30 (D) si les vérifications des étapes (B) et (C) sont satisfaites, désactivation des moyens de verrouillage programmables de la carte.

Avantageusement, le procédé de programmation peut présenter au moins l'une des caractéristiques optionnelles suivantes :

- les informations dont la correspondance est
5 vérifiée à l'étape (B) comprennent au moins l'une parmi un code confidentiel saisi sur des moyens de saisie du dispositif de sécurisation, et une clé d'identification enregistrée dans les deuxièmes moyens de stockage du dispositif de sécurisation, comparée avec une clé
10 stockée dans la puce de la carte.

- le procédé comprend l'étape supplémentaire suivante :

(E) si les vérifications sont satisfaites, initialiser la valeur de compteur de la carte à un
15 nombre d'opérations autorisées par défaut.

- le procédé comprend l'étape supplémentaire suivante :

(F) saisie par le porteur d'un nombre d'opérations autorisées voulues et initialisation de la valeur de
20 compteur de la carte avec ce nombre saisi.

On prévoit enfin, selon l'invention, un procédé d'enrôlement d'un dispositif de sécurisation et d'une carte tels que respectivement définis plus haut, mis en
25 œuvre dans un système comportant un processeur, des moyens de stockage, des moyens de connexion, et une base de données mémorisée dans les moyens de stockage, le procédé comportant des étapes de :

(A) branchement du dispositif de sécurisation aux
30 moyens de connexion du système,

(B) insertion de la carte dans le dispositif de sécurisation,

(C) création d'une fiche dans la base de données associant le porteur, la carte et le dispositif de sécurisation,

(D) enregistrement dans les premiers moyens de
5 stockage du dispositif de sécurisation des paramètres biologiques du porteur relevés à l'aide des moyens d'évaluation de paramètres biologiques du dispositif de sécurisation.

10 Avantageusement, le procédé d'enrôlement peut présenter au moins l'une des caractéristiques optionnelles suivantes :

 - le procédé comprend, préalablement à l'étape (C),
une étape de génération et/ou lecture de la clé
15 d'identification dans les deuxièmes moyens de stockage du dispositif de sécurisation, ainsi que l'étape supplémentaire suivante :

(E) enregistrement de la clé d'identification du
dispositif de sécurisation dans les moyens de stockage
20 de la puce de la carte.

 - une fois lue, la clé d'identification est chiffrée puis enregistrée dans la base de données.

D'autres caractéristiques, buts et avantages de
25 l'invention apparaîtront à la lecture ci-après d'un mode de réalisation préférentiel de l'invention. Aux dessins annexés, la figure 1 présente un dispositif de sécurisation selon l'invention associé avec une carte à puce selon l'invention.

30

En référence à la figure 1, une carte 1 dite "carte à puce" est de forme rectangulaire et présente une épaisseur de 1mm environ. Sur une de ses faces

principales, un emplacement est réservé à la puce (non représentée) ainsi qu'à une connectique d'interface 3. Cette connectique d'interface 3 est ici constituée de plusieurs contacts 4 de cuivre ou tout autre matériau 5 conducteur de signal électrique.

Un dispositif de sécurisation 2, appelé aussi par la suite étui, se présente sous les dimensions et l'aspect général d'une calculatrice dite de poche. Elle 10 comprend une fente 8 pour la réception de la carte 1, ici située sur l'un des côtés de l'étui 2. Sur une face supérieure, l'étui 2 présente un écran d'affichage 6 qui est, de préférence, un affichage de type à cristaux liquides connu en soi, apte à afficher des informations 15 à destination de l'utilisateur. Des moyens de saisie 7 sont présents sous les moyens d'affichage 6. Ces moyens de saisie sont constitués ici de touches. De préférence, les moyens de saisie sont équivalents à ceux d'une calculatrice de base comprenant les 10 chiffres de 0 à 20 9, le point formant virgule, les quatre opérations de base que sont l'addition, la soustraction, la multiplication et la division, le signe égal. Optionnellement, les moyens de saisie comportent en outre une touche permettant le calcul du pourcentage, 25 des touches de mémorisation et d'opérations d'addition et de soustraction sur la mémoire. La mise en route de l'étui 2 s'effectue lors de l'insertion de la carte dans la fente de réception 8, le retrait de la carte éteignant l'étui 2.

30

L'étui 2 comporte, sous les moyens de saisie 7, des moyens de détection de paramètres biologiques 5. Ces moyens de détection de paramètres biologiques

comprennent de préférence un capteur d'empreintes digitales. Cependant, il est possible que les moyens de détection de paramètres biologiques comprennent un microphone apte à enregistrer la voix du porteur dans le
5 but de réaliser une reconnaissance vocale, ou encore un capteur d'empreinte rétinienne. D'autres moyens de détection de paramètres biologiques peuvent être utilisés.

10 A l'intérieur de l'étui 2, un circuit électronique comporte un processeur ainsi que des moyens de mémorisation. Les moyens de mémorisation sont aptes à mémoriser localement des paramètres biologiques du porteur tels que ses empreintes digitales. Le processeur
15 est apte à mettre en œuvre un logiciel d'acquisition et d'analyse d'empreintes digitales. Le logiciel est apte, d'autre part, à comparer une empreinte digitale acquise sur le capteur d'empreintes digitales 5 avec les empreintes digitales mémorisées dans les moyens de
20 mémorisation.

Le dispositif de sécurisation 2 comporte enfin des moyens de connexion (non représentés) à un système informatique externe. Ces moyens de connexion peuvent se
25 brancher de manière préférentielle sur un port USB du système informatique externe (USB, acronyme du terme anglo-saxon "Universal Serial Bus", signifiant "Bus Série Universel") ou encore sur un port série ou parallèle dudit système informatique, ou encore sur un
30 port dit "Firewire".

La puce de la carte 1 comporte des moyens de verrouillage programmables par le dispositif de

sécurisation 2. Ces moyens de verrouillage programmables sont aptes à permettre d'auto-verrouiller la carte à puce sous certaines conditions, comme on le verra plus loin. D'autre part, la puce comporte une première zone
5 de mémoire protégée contenant la valeur de compte d'un compteur mis en œuvre par le processeur. Ce compteur est apte à comptabiliser le nombre de transactions ou opérations effectuées avec la carte à puce. D'une manière préférentielle, le compteur est initialisé avec
10 un nombre d'opérations autorisées. A chaque fois qu'une opération est effectuée, le compteur est décrémenté d'une opération. D'autre part, la puce comporte une seconde zone de mémoire protégée dans laquelle est mémorisée une clé d'identification qui sert à la
15 programmation de la carte à puce avec un dispositif de sécurisation unique 2 comportant lui aussi des moyens de stockage d'une clé d'identification similaire. De manière générale, à chaque fois que la carte à puce est introduite dans le dispositif de sécurisation 2, la
20 carte effectue une vérification de la clé d'identification enregistrée dans les moyens de stockage de celui-ci.

On va maintenant décrire l'utilisation de la carte
25 à puce selon l'invention. On suppose la carte à puce non verrouillée et le compteur de la carte à puce initialisé à N opérations autorisées (N supérieur ou égal à 1). Une telle carte à puce, ainsi configurée, est utilisée de manière courante comme toute carte à puce standard. Elle
30 est introduite, lors d'un achat, dans un TPE (Terminal de Paiement Electronique) sur lequel le porteur est invité à saisir son code confidentiel pour valider la transaction. Si le code confidentiel entré par le

porteur est valable, la transaction est validée et le compteur d'opérations autorisées est décrémenté d'une unité. Si le compteur est égal à zéro, cela signifie qu'aucune opération n'est plus autorisée sur cette carte
5 à puce, et les moyens de verrouillage programmables s'auto-activant en empêchant toute transaction ultérieure avec la carte.

Si le porteur de la carte a saisi lors d'une
10 transaction un code confidentiel erroné (une fois ou préférentiellement trois fois de suite), le compteur de transaction est soit décrémenté, soit forcé à zéro par la carte. De nouveau, si le compteur est égal à zéro, la carte à puce est inutilisable pour toute transaction
15 ultérieure.

On va maintenant décrire la coopération de l'étui 2 avec la carte à puce 1. Dans cette coopération, l'étui 2 sert principalement à programmer les moyens de
20 verrouillage programmables de la carte ainsi que le nombre d'opérations autorisées enregistrées dans le compteur. Une fois la carte à puce insérée dans la fente de réception 8 de l'étui 2, la carte effectue une comparaison entre sa clé d'identification et celle
25 enregistrée dans la mémoire de stockage de l'étui. Si cette vérification échoue, l'étui 2, via les moyens d'affichage, indique au porteur que la carte à puce insérée n'est pas appariée avec le dispositif. Si les clés concordent, l'étui commence par forcer le compteur
30 de la carte à puce à zéro, rendant cette dernière inopérante pour la suite. De la sorte, si la procédure est interrompue à ce stade, la carte à puce est inutilisable. Toujours dans l'hypothèse où les clés

concordent, le dispositif de sécurisation 2 affiche un message demandant au porteur de placer l'un de ses doigts sur le capteur d'empreintes 5. Dès lors l'étui 2 met en œuvre, à l'aide de son processeur et de son circuit électronique, le logiciel d'acquisition d'empreintes digitales pour relever l'empreinte du doigt placé sur le capteur 5. Ensuite, via le logiciel, il effectue une comparaison de cette empreinte relevée avec celles qu'il a en mémoire. S'il y a concordance entre l'une des empreintes mémorisées et celle relevée sur le capteur, le dispositif de sécurisation 2 effectue un déverrouillage de la carte, en désactivant les moyens de verrouillage programmables de la carte et en initialisant par défaut le compteur d'opérations autorisées à 1. Ensuite, de manière préférentielle, le dispositif de sécurisation 2 demande au porteur le nombre de transactions autorisées avec lequel il désire initialiser le compteur de la carte à puce. Le porteur saisit alors le nombre de son choix (avec de préférence un plafond) et le valide, et la valeur du compteur est fixée à ce nombre.

Si l'empreinte lue sur le capteur 5 ne correspond à aucune des empreintes enregistrées par le dispositif de sécurisation 2, ce dernier indique sur les moyens d'affichage une erreur lors de la reconnaissance et laisse la carte à puce dans un état verrouillé, avec le compteur à zéro.

De manière optionnelle, l'étui 2 peut servir de calculatrice de base pour des opérations simples d'addition, de soustraction, de multiplication et de division ainsi que de pourcentage. De plus, l'étui 2

peut permettre au porteur de lire les informations accessibles contenues dans la carte à puce, comme l'historique des transactions ou le solde d'un portemonnaie électronique lorsqu'une telle fonction est
5 implémentée dans la carte 1.

On va maintenant décrire un procédé d'enrôlement ou d'appariement qui permet d'appareiller un dispositif de sécurisation 2 avec une carte à puce 1 de manière
10 unique. De préférence, cette opération d'enrôlement ne peut être effectuée qu'au sein d'une agence bancaire à l'aide d'une machine dite de banque qui est un système informatique de type connu en soi, mettant en œuvre un logiciel particulier incluant le procédé qui va être
15 décrit. Pour effectuer cet enrôlement, le dispositif de sécurisation 2 est connecté au système informatique de la machine de banque via notamment un port USB, un port série, un port parallèle ou encore un port de type "Firewire". Ensuite, la carte à puce est insérée dans la
20 fente 8 de réception de l'étui 2. Le système informatique effectue une lecture de la clé d'identification du dispositif de sécurisation 2. Puis il chiffre cette clé à l'aide d'un algorithme de chiffrement connu seulement de la machine de banque.
25 Ensuite, le système informatique de la machine de banque crée un nouvel enregistrement dans une base de données mémorisée dans ledit système, enregistrement qui associe le porteur avec le dispositif de sécurisation 2 et la carte à puce 1 de manière unique. Ensuite le procédé
30 effectue une vérification des données requises contenues dans cette fiche. Puis le procédé effectue la mémorisation des empreintes digitales du porteur dans la mémoire du dispositif de sécurisation 2. Pour cela, on

utilise soit le capteur d'empreintes digitales 5 du dispositif de sécurisation, soit un système de reconnaissance d'empreintes digitales directement intégré à la machine de banque. Enfin, le procédé écrit 5 dans la zone protégée de la carte à puce la clé d'identification, pour ainsi achever l'enrôlement entre le porteur, le dispositif de sécurisation 2 et la carte à puce 1.

10 Il est à noter que seul le dispositif de sécurisation 2 mémorisant les empreintes digitales du porteur est capable de verrouiller et de déverrouiller la carte à puce 1. La perte, le vol ou le bris du dispositif de sécurisation 2 nécessite soit de remplacer 15 la carte à puce, soit d'effectuer un nouvel appariement de la carte à puce 1 avec un nouveau dispositif de sécurisation 2 à l'aide de la machine de banque en utilisant le procédé d'enrôlement précité.

20 Il est à noter aussi que les empreintes digitales peuvent ne pas être stockées dans la machine de banque ayant servi à l'enrôlement, ces empreintes restant la propriété exclusive du porteur.

25 Bien entendu, on pourra apporter à l'invention de nombreuses modifications et variantes.

REVENDICATIONS

1. Dispositif (2) de sécurisation d'une carte à puce
5 (1), caractérisé en ce qu'il comprend des moyens
d'évaluation de paramètres biologiques (5) d'un porteur
de la carte aptes à sélectivement autoriser la
modification d'une valeur de compteur de la carte à puce
pour un nombre déterminé d'opérations autorisées, de
10 manière à déverrouiller ou à verrouiller la carte à
puce.

2. Dispositif selon la revendication 2, caractérisé en
ce que les moyens d'évaluation de paramètres biologiques
15 comprennent un capteur d'empreintes digitales (5).

3. Dispositif selon la revendication 1 ou 2,
caractérisée en ce que les moyens d'évaluation de
paramètres biologiques comportent des premiers moyens de
20 stockage aptes à mémoriser les paramètres biologiques du
porteur.

4. Dispositif selon l'une des revendications 1 à 3,
caractérisé en ce qu'il comporte des deuxièmes moyens de
25 stockage aptes à mémoriser une clé d'identification.

5. Carte (1), notamment carte bancaire, comportant une
puce électronique ainsi que des moyens d'interfaçage (3)
de la puce, caractérisée en ce que la puce comprend,
30 dans une zone à accès contrôlé, une valeur de compteur
de nombre d'opérations autorisées, capable d'être
modifiée lors d'une transmission d'informations par les
moyens d'interfaçage, et des moyens de verrouillage

aptes à verrouiller la carte lorsque la valeur de compteur atteint un seuil, la valeur de compteur pouvant être initialisée par une information spécifique transmise par les moyens d'interfaçage.

5

6. Carte selon la revendication 5, du type associé à un code confidentiel, caractérisée en ce qu'elle comprend des moyens aptes, lors de la réception dans la carte d'un code confidentiel erroné, à modifier la
10 valeur de compteur, notamment à forcer ladite valeur à la valeur du seuil.

7. Carte selon la revendication 5 ou 6, caractérisée en ce qu'elle comprend des moyens aptes, lors de la
15 réception d'une information de validation d'une transaction effectuée, à modifier la valeur de compteur.

8. Carte selon l'une des revendications 5 à 7, caractérisée en ce que la puce comporte des moyens de
20 stockage d'une clé d'identification.

9. Carte selon la revendication 8, caractérisée en ce que la clé d'identification est apte à autoriser le déverrouillage de la carte et/ou une initialisation de
25 la valeur de compteur via les moyens d'interfaçage.

10. Carte selon l'une des revendications 5 à 9, caractérisé en ce que les moyens d'interfaçage de la puce sont aptes à coopérer avec un dispositif de
30 sécurisation selon l'une des revendications 1 à 4.

11. Procédé de programmation pour un dispositif de sécurisation selon l'une des revendications 1 à 4, caractérisé en ce qu'il comprend les étapes suivantes :

5 (A) insertion de la carte dans le dispositif de sécurisation,

(B) vérification de la correspondance entre une information contenue dans le dispositif de mémorisation et une information contenue dans la puce de la carte,

10 (C) vérification des paramètres biologiques du porteur par les moyens d'évaluation de paramètres biologiques du dispositif de sécurisation,

(D) si les vérifications des étapes (B) et (C) sont satisfaites, désactivation des moyens de verrouillage programmables de la carte.

15

12. Procédé de programmation selon la revendication 11, caractérisé en ce que les informations dont la correspondance est vérifiée à l'étape (B) comprennent au moins l'une parmi un code confidentiel saisi sur des
20 moyens de saisie (7) du dispositif de sécurisation, et une clé d'identification enregistrée dans les deuxièmes moyens de stockage du dispositif de sécurisation, comparée avec une clé stockée dans la puce de la carte.

25 13. Procédé de programmation selon la revendication 11 ou 12, caractérisé en ce qu'il comprend l'étape supplémentaire suivante :

(E) si les vérifications sont satisfaites, initialiser la valeur de compteur de la carte à un
30 nombre d'opérations autorisées par défaut.

14. Procédé de programmation selon l'une des revendications 11 à 13, caractérisé en ce qu'il comprend l'étape supplémentaire suivante :

(F) saisie par le porteur d'un nombre d'opérations autorisées voulues et initialisation de la valeur de compteur de la carte avec ce nombre saisi,

15. Procédé d'enrôlement d'un dispositif de sécurisation selon l'une des revendications 1 à 4 et d'une carte selon l'une des revendications 5 à 10, mis en œuvre dans un système comportant un processeur, des moyens de stockage, des moyens de connexion, et une base de données mémorisée dans les moyens de stockage, le procédé comportant des étapes de :

(A) branchement du dispositif de sécurisation aux moyens de connexion du système,

(B) insertion de la carte dans le dispositif de sécurisation,

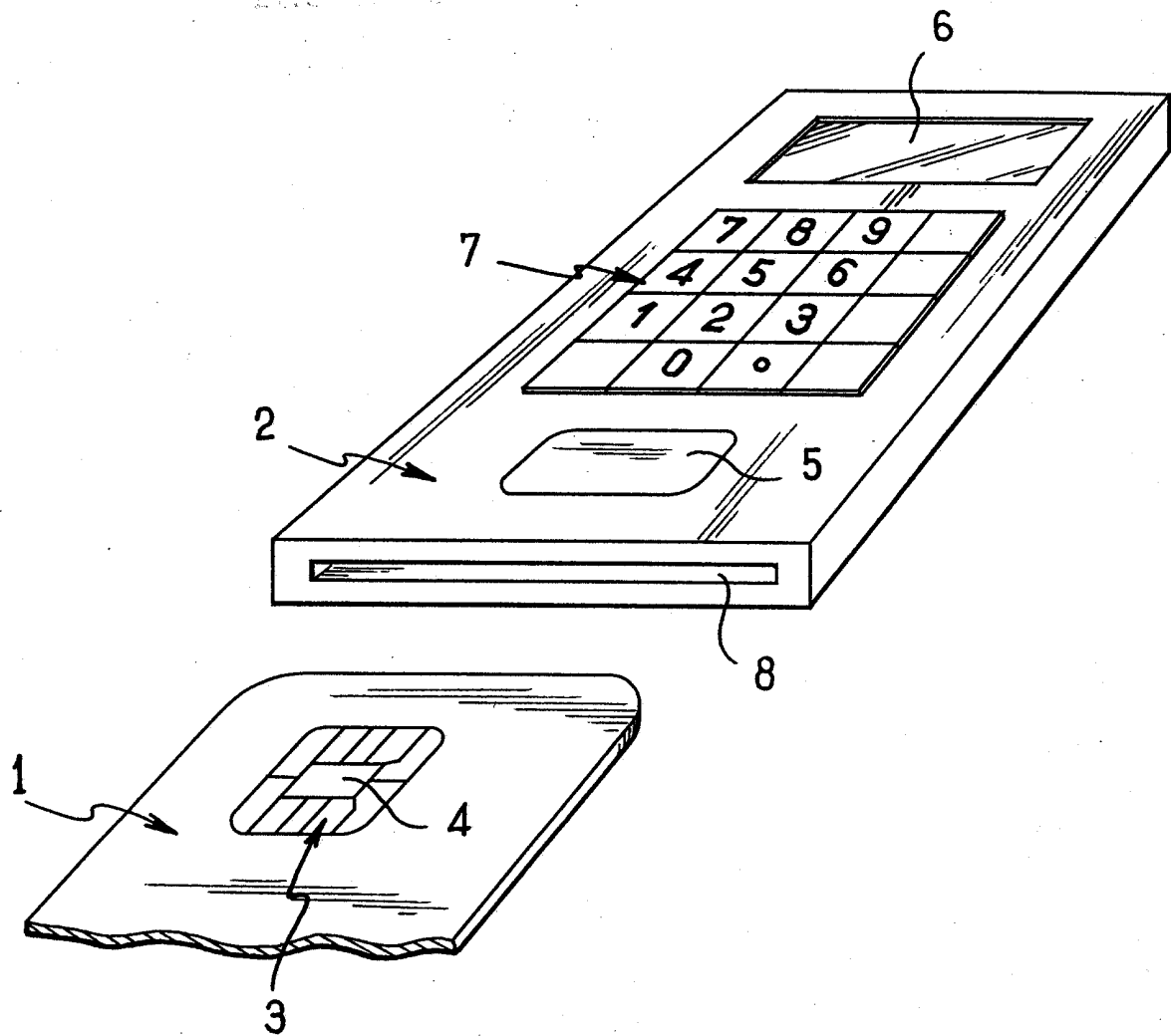
(C) création d'une fiche dans la base de données associant le porteur, la carte et le dispositif de sécurisation,

(D) enregistrement dans les premiers moyens de stockage du dispositif de sécurisation des paramètres biologiques du porteur relevés à l'aide des moyens d'évaluation de paramètres biologiques du dispositif de sécurisation.

16. Procédé d'enrôlement selon la revendication 15, caractérisé en ce qu'il comprend, préalablement à l'étape (C), une étape de génération et/ou lecture de la clé d'identification dans les deuxièmes moyens de stockage du dispositif de sécurisation, ainsi que l'étape supplémentaire suivante :

(E) enregistrement de la clé d'identification du dispositif de sécurisation dans les moyens de stockage de la puce de la carte.

- 5 17. Procédé d'enrôlement selon la revendication 16, caractérisé en ce que, une fois lue, la clé d'identification est chiffrée puis enregistrée dans la base de données.

FIG. 1

**RAPPORT DE RECHERCHE
PRÉLIMINAIRE**

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

FA 616313
FR 0116994

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	US 4 879 645 A (OZAKI HIROSHI ET AL) 7 novembre 1989 (1989-11-07) * revendication 1; figures 2,4,6 *	5,7	G06K19/07 G06K7/00 G06K9/00
X	EP 1 085 424 A (YASUKURA YUTAKA) 21 mars 2001 (2001-03-21)	15	
A	* alinéa '0164! - alinéa '0171! * * revendication 1; figures 1-6 *	11,12	
Y	US 5 907 149 A (MARCKINI EUGENE F) 25 mai 1999 (1999-05-25) * colonne 2, ligne 6 - ligne 46 * * revendications 1,3-6,8; figures *	1-4,10	
Y	US 6 219 439 B1 (BURGER PAUL M) 17 avril 2001 (2001-04-17) * colonne 5, ligne 6 - ligne 24 * * revendications 1-4; figures *	1-4,10	
A	EP 0 973 134 A (IBM) 19 janvier 2000 (2000-01-19) * alinéa '0018! - alinéa '0020! * * revendications 1,2,4; figure 1 *	1-4	DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7) G07F G07C
A	FR 2 765 985 A (GEMPLUS CARD INT) 15 janvier 1999 (1999-01-15) * revendications 1,7,10; figures 2,3 *	1-4	
A	FR 2 786 006 A (SCHLUMBERGER SYSTEMS & SERVICE) 19 mai 2000 (2000-05-19) * page 2, ligne 13 - ligne 31 * * page 5, ligne 6 - ligne 19 * * revendications 1-5; figures 1,2 *	1-4	
Date d'achèvement de la recherche		Examineur	
7 novembre 2002		Paraf, E	
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 0116994 FA 616313**

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 07-11-2002
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
US 4879645 A	07-11-1989	JP 60207957 A	19-10-1985
		DE 3580778 D1	17-01-1991
		EP 0157303 A2	09-10-1985
EP 1085424 A	21-03-2001	JP 3112076 B2	27-11-2000
		JP 11338826 A	10-12-1999
		AU 3848999 A	06-12-1999
		EP 1085424 A1	21-03-2001
		CN 1272188 T	01-11-2000
		WO 9960485 A1	25-11-1999
US 5907149 A	25-05-1999	AUCUN	
US 6219439 B1	17-04-2001	AUCUN	
EP 0973134 A	19-01-2000	DE 19831884 A1	20-01-2000
		CN 1245311 A	23-02-2000
		EP 0973134 A1	19-01-2000
		JP 2000047945 A	18-02-2000
		KR 2000011286 A	25-02-2000
FR 2765985 A	15-01-1999	FR 2765985 A1	15-01-1999
		AU 8545398 A	08-02-1999
		EP 0995175 A1	26-04-2000
		WO 9903074 A1	21-01-1999
		JP 2002511610 T	16-04-2002
FR 2786006 A	19-05-2000	FR 2786006 A1	19-05-2000
		AU 1051300 A	05-06-2000
		CN 1326580 T	12-12-2001
		EP 1131799 A1	12-09-2001
		WO 0030047 A1	25-05-2000
		JP 2002530758 T	17-09-2002

EPO FORM P0465