



DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

<p>(51) Classification internationale des brevets <sup>6</sup> : <b>G07F 7/10</b></p>	<p><b>A1</b></p>	<p>(11) Numéro de publication internationale: <b>WO 99/03074</b> (43) Date de publication internationale: 21 janvier 1999 (21.01.99)</p>
<p>(21) Numéro de la demande internationale: PCT/FR98/01464 (22) Date de dépôt international: 8 juillet 1998 (08.07.98) (30) Données relatives à la priorité: 97/08813 10 juillet 1997 (10.07.97) FR (71) Déposant (pour tous les Etats désignés sauf US): GEMPLUS S.C.A. [FR/FR]; Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F-13881 Gémenos Cedex (FR). (72) Inventeurs; et (75) Inventeurs/Déposants (US seulement): JEAN, Lionel [FR/FR]; 12, rue des Bons Amis, F-13012 Marseille (FR). OUVRAY, Jean, Claude [FR/FR]; La Petite Chartreuse, 17, avenue Standal, F-13009 Marseille (FR). (74) Mandataire: NONNENMACHER, Bernard; Gemplus S.C.A., Parc d'Activités de Gémenos, Avenue du Pic de Bertagne, F-13881 Gémenos Cedex (FR).</p>		<p>(81) Etats désignés: AL, AU, BA, BB, BG, BR, CA, CN, CU, CZ, EE, GE, HU, ID, IL, IS, JP, KP, KR, LC, LK, LR, LT, LV, MG, MK, MN, MX, NZ, PL, RO, SG, SI, SK, SL, TR, TT, UA, US, UZ, VN, YU, brevet ARIPO (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).</p> <p>Publiée Avec rapport de recherche internationale. Avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues.</p>

(54) Title: METHOD FOR MANAGING A SECURE TERMINAL

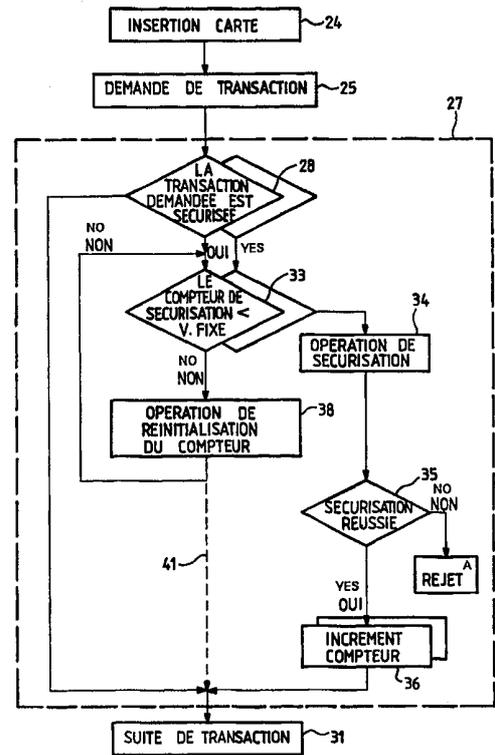
(54) Titre: PROCEDE DE GESTION D'UN TERMINAL SECURISE

(57) Abstract

The invention concerns a method solving security problems resulting from the addition of a security circuit to a smart card reading terminal by providing said security circuit with means for counting (36) the number of times (34) the security circuit is activated for certain sensitive operations. When the total of said operations reaches a fixed value (33), the security circuit is prevented from operating until it is re-initialised (38) again. Optionally the circuit may have to be replaced by another.

(57) Abrégé

On résout les problèmes de sécurité résultant de l'adjonction d'un circuit de sécurité à un terminal de lecture de carte à puce en prévoyant, pour ce circuit de sécurité de compter (36) le nombre d'occasions (34) de sollicitation de ce circuit de sécurité pour effectuer certaines opérations sensibles. Lorsque le compte de ces opérations atteint une valeur fixée (33) on empêche ce circuit de sécurité de fonctionner jusqu'à sa prochaine ré-initialisation (38). Eventuellement on peut être amené à devoir remplacer le circuit par un autre.



- 24...INSERTING CARD
- 25...REQUESTING TRANSACTION
- 28...REQUESTED TRANSACTION IS MADE SECURE
- 32...SECURITY COUNTER < FIXED VALUE
- 34...SECURITY OPERATION
- 36...COUNTER INCREMENT
- 38...RE-INITIALISING COUNTER
- 35...SECURITY ENSURED
- 31...TRANSACTION CONTINUED
- A...REJECTED

**UNIQUEMENT A TITRE D'INFORMATION**

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce	ML	Mali	TR	Turquie
BG	Bulgarie	HU	Hongrie	MN	Mongolie	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MR	Mauritanie	UA	Ukraine
BR	Brésil	IL	Israël	MW	Malawi	UG	Ouganda
BY	Bélarus	IS	Islande	MX	Mexique	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	NE	Niger	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NL	Néerlande	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norvège	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NZ	Nouvelle-Zélande	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	PL	Pologne		
CM	Cameroun	KR	République de Corée	PT	Portugal		
CN	Chine	KZ	Kazakstan	RO	Roumanie		
CU	Cuba	LC	Sainte-Lucie	RU	Fédération de Russie		
CZ	République tchèque	LI	Liechtenstein	SD	Soudan		
DE	Allemagne	LK	Sri Lanka	SE	Suède		
DK	Danemark	LR	Libéria	SG	Singapour		
EE	Estonie						

## PROCEDE DE GESTION D'UN TERMINAL SECURISE

La présente invention a pour objet un procédé de gestion d'un terminal sécurisé dit aussi lecteur, ainsi qu'un circuit de sécurité pour la mise en oeuvre du procédé. Elle concerne le domaine des cartes à microcircuit dites à puces et plus généralement le domaine des objets portables à puce. Ce domaine est celui par lequel avec des circuits électroniques soit on authentifie des porteurs de cartes à puce, soit on authentifie des contenus d'informations que contiennent les mémoires de ces cartes, soit enfin on effectue des paiements, ou des augmentations de crédits, en modifiant un nombre mémorisé dans la carte et représentatif d'unités de paiement ou de points de fidélité.

L'invention a pour objet, devant le développement très important des transactions accessibles avec des cartes à puces, de rendre plus sûr, de sécuriser, les terminaux de lecture, dont le nombre disponible croît parallèlement aux utilisations des cartes à puces.

Un procédé de gestion de transactions utilisant des cartes à puce, est par exemple décrit dans la demande de brevet Européen EP-A-91 400 201.9 déposée le 29.01.1991.

Les systèmes de sécurité actuellement en vigueur comportent, dans les lecteurs, des circuits de sécurité dont la tâche est notamment de contrôler l'exécution de tous ces protocoles de vérification ou d'authentification exécutables par le lecteur. Ces circuits de sécurité, appelés circuit SAM dans la littérature anglo-saxonne (SECURE APPLICATION MICROMODULE), sont généralement amovibles et sont

connectés au lecteur pour d'une part assurer ce  
contrôle des opérations de sécurité, et d'autre part  
préciser certaines opérations liées à une application  
particulière mise en oeuvre par le lecteur. Une  
5 application est une série d'opérations exécutées par un  
lecteur, ou un appareil auquel ce lecteur est relié, et  
qui amènent à la satisfaction d'un besoin (en biens ou  
en services) exprimé par le porteur de la carte. Le  
caractère amovible de ces circuits de sécurité les rend  
10 fragiles vis-à-vis des fraudeurs dont on soupçonne  
qu'il voudront en connaître le secret. Ceci sera  
d'autant plus réalisable que le nombre de circuits de  
sécurité sera grand.

Un des but de l'invention est de garantir que les  
15 terminaux et les modules de sécurité ne soient pas  
utilisés en dehors de l'application à laquelle il sont  
dédiés. En effet, l'utilisation illégale d'un circuit  
de sécurité, sans terminal, est critique du point de  
vue de la sécurité car il est possible à un fraudeur  
20 d'avoir des informations sur les secrets contenus dans  
le circuit de sécurité. L'utilisation d'un terminal  
sans son circuit de sécurité est généralement sans  
intérêt car le terminal ne détient pas les secrets de  
l'application. Il n'est donc pas capable de faire grand  
25 chose. L'utilisation d'un terminal et de son circuit de  
sécurité est par ailleurs dans certains cas elle aussi  
critique. En effet l'ensemble terminal plus circuit de  
sécurité permet de réaliser des opérations complètes  
sur de vraies cartes. Il est donc indispensable de  
30 limiter l'utilisation des circuits de sécurité seuls et  
des ensembles circuit de sécurité plus terminal.

Dans l'invention, pour remédier aux problèmes  
cités, on préconise de compter le nombre de fois où le  
circuit de sécurité est utilisé pour des commandes

dites sensibles. On considérera comme commandes sensibles des commandes permettant notamment de donner des droits d'accès, d'authentifier, de garantir la confidentialité, de produire des cryptogrammes, de  
5 vérifier des certificats, etc... D'une manière générale, toute commande pourra être à considérer comme sensible. Dans ce cas son existence sera assortie d'un attribut qui lui donne ou non ce caractère.

Dans l'invention, lorsque le compte du nombre  
10 d'utilisations du circuit de sécurité atteint une valeur fixée, on bloque le fonctionnement de ce circuit de sécurité. Dans ce cas, ce circuit de sécurité ne peut plus effectuer son travail de sécurité. Dans ces conditions, à chaque fois qu'il est sollicité par le  
15 terminal, les transactions menées par le terminal, et pour lesquelles son fonctionnement est requis sont bloquées. Dans un perfectionnement bien entendu le compteur de ce circuit de sécurité peut être ré-initialisé en respectant une procédure qui elle-même  
20 est sécurisée.

L'invention a donc pour objet un procédé de gestion d'un terminal sécurisé utilisé pour des transactions avec des cartes à puce comportant les étapes suivantes

- on met une carte à puce en relation avec le  
25 terminal,

- on fait exécuter un programme par le terminal, ce programme comportant des actions sensibles relatives à la sécurisation des transactions,  
caractérisé en ce que

30 - on compte le nombre de fois où le terminal est sollicité pour exécuter des opérations sensibles, et

- on limite l'action de ce terminal dès que ce compte atteint une valeur fixée.

Au sens de l'invention, il peut y avoir sollicitation dès la réception et identification par le terminal ou le module de sécurité d'une instruction ou d'une commande sensible. Il est donc possible de  
5 comptabiliser les commandes sensibles indépendamment de leur exécution et/ou du résultat de leur exécution.

L'invention a également pour objet un circuit de sécurité pour la mise en oeuvre du procédé ci-dessus. Il est caractérisé en ce qu'il comporte des moyens de  
10 gestion aptes à identifier et comptabiliser des sollicitations provenant de l'extérieur et à limiter ses fonctions dès que la comptabilisation atteint un nombre prédéterminé. Les sollicitations peuvent  
15 provenir soit du terminal, soit du système maître, soit d'un émulateur de terminal qui serait réalisé par un fraudeur.

L'invention sera mieux comprise à la lecture de la description qui suit et à l'examen des figures qui l'accompagnent. Celles-ci ne sont données qu'à titre  
20 indicatif et nullement limitatif de l'invention. Les figures montrent:

- figure 1: une représentation schématique d'un terminal utilisable pour mettre en oeuvre le procédé de l'invention;
- 25 - figure 2: un organigramme montrant les principales étapes du procédé de l'invention;
- figure 3: l'architecture des moyens électroniques mis en oeuvre dans le terminal de la figure 1;
- figure 4: un exemple d'opération sensible de  
30 sécurité effectuée par le circuit de sécurité de l'invention.

La figure 1 montre un terminal 1 utilisable pour mettre en oeuvre le procédé de l'invention. Le terminal 1 comporte d'une manière connue, de préférence, un

clavier 2, un écran 3 et une fente 4 pour y introduire une carte 5 à puce à lire avec le terminal lecteur 1. Le terminal 1 peut par ailleurs être en relation avec un système maître 6. La relation peut notamment être du type télécommunication, le système maître 6 étant distant. Les télécommunications peuvent par exemple être hertziennes. Le terminal 1 est cependant apte à effectuer un certain nombre d'opérations de manière autonome et c'est de celles-ci dont il est principalement question. Dans un exemple particulier montré sur la figure 1, le circuit de sécurité utilisable dans le terminal 1 est amovible: c'est un circuit 7 enchâssé dans un objet 8 portable à puce. L'objet 8 portable à puce peut avoir la même forme qu'une carte à puce 5. De préférence, il a une forme différente avec notamment une partie géométrique de détrompage 9 pour empêcher les utilisateurs de mal le placer. L'objet 8 est destiné à être introduit dans une fente 10 de lecture du terminal 1 destiné à le recevoir lui seul.

La figure 3, montrée en dessous de la figure 1, montre pour les parties correspondantes l'architecture du système électronique ainsi constitué. Le circuit 7 comporte ainsi, de préférence, un micro-processeur 11 en relation par un bus d'adresses de données et de commande 12, d'une part avec une interface d'entrée sortie 13 représentée par un connecteur. Le micro-processeur est d'autre part en relation avec un jeu de mémoires 14 et 15 et de compteurs 16 et 17.

De la même façon, le système électronique du lecteur 1 comporte un micro-processeur 18 en relation avec un bus 19, du même type que le bus 12, avec deux interfaces d'entrée-sortie respectivement 20 et 21 pour communiquer avec le circuit 7 d'une part, et avec un

microcircuit électronique 22 de la carte à puce 5 d'autre part. Le bus 19 est encore en relation avec le clavier 2 et l'écran 3. Le micro-processeur 18 exécute par ailleurs des programmes qui sont contenus dans une  
5 mémoire programme 23.

Les structures physiques des micro-processeurs, des mémoires programmes, des bus et des interfaces peuvent être variées. De préférence, les mémoires sont des mémoires de type non volatiles. Les compteurs 16 et 17  
10 sont des compteurs non volatiles. Ils peuvent être réalisés à la méthode d'un boulier: chaque incrémentation du compteur revenant à faire changer d'état une des cellules mémoires d'un registre, servant de boulier, et jouant le rôle de compteur. Lorsque  
15 toutes les cellules mémoires ont basculé, le compteur a atteint la valeur fixée. De préférence néanmoins, le compteur pourra être réalisé sous la forme d'une enregistrement enregistré en une mémoire 50 de données associée à un logiciel de comptage du circuit 7. Le  
20 logiciel de comptage consistant, à chaque incrément, à aller lire la valeur ancienne du compteur, à incrémenter sa valeur d'unités, et à inscrire à la place de cet enregistrement la nouvelle valeur du compteur. Dans ce cas, la valeur fixée est contenue  
25 dans le logiciel de comptage. De plus, les clavier 2 et écran 3 ne sont nécessaires que dans la mesure où l'application mise en oeuvre par le terminal 1 requiert la visualisation et la saisie de l'information du porteur de la carte. Dans certains cas, ils peuvent  
30 être omis, le protocole d'échange entre la carte 5 et le terminal 1 étant automatique.

La figure 2 montre les étapes principales du procédé de gestion de l'invention. Au cours d'une étape 24 un opérateur met une carte à puce 5 en relation avec

le terminal 1. Le terminal 1, en application des instructions de son programme 26 mémorisé dans la mémoire 23, et exécuté par le micro-processeur 18 réagit à cette insertion et effectue une demande de transaction 25. Cette demande de transaction peut être  
5 simplement la configuration du micro-processeur 18 pour le mettre à la disposition du micro-processeur 11. La demande de transaction peut ainsi, par exemple dans le cas de la vérification du porteur d'une carte à puce,  
10 être la demande de vérification du code secret de ce porteur. Dans ce cas, le programme 26 mémorisé dans la mémoire 23 comporte une instruction du type: "Lancement de l'opération de vérification du code secret du titulaire par le circuit de sécurité 7". Cette demande  
15 de transaction adressée par le microprocesseur 18 au microprocesseur 11 peut néanmoins être différente et correspondre à toutes les opérations de sécurité évoquées ci-dessus.

Selon l'invention, le circuit de sécurité 7 effectue alors la suite des opérations 27 de la figure  
20 2. Au cours d'une première opération 28 de cette suite 27, le micro-processeur 11 du circuit 7 regarde si une instruction 29 de son programme 30 de sécurité chargé en mémoire 14, est une instruction de type sensible ou  
25 non. Elle est du type sensible, si elle est affectée par exemple d'un attribut, d'un drapeau, qui lui est associé à cet effet. Un tel drapeau peut par exemple être une configuration particulière de bits du code instruction de l'instruction 29.

30 Si elle n'est pas une instruction de type sensible, si elle n'est pas du type pour lequel il faut compter le nombre de fois où elle a été mise en oeuvre, la suite de la transaction est immédiate. Le circuit 7 et/ou le lecteur 1 continuent alors, par l'opération 31

à fonctionner comme dans l'état de la technique. Par contre, si l'opération demandée relative à l'instruction 29 est une opération sensible, le microprocesseur 11 intercale dans le déroulement du programme 30 un programme 32 de gestion du compteur mémorisé lui aussi dans la mémoire 14. Dans le programme 32 il y a un premier test 33 par lequel on cherche à savoir si un compteur de sécurité, par exemple le compteur 16, comporte une valeur inférieure à une valeur fixée d'avance. Si c'est le cas, l'opération de sécurisation 34 impliquée par l'instruction 29 est exécutée. D'une manière classique le programme 30 comporte une vérification 35 de ce que l'opération 34 a été réussie. Si au cours du test 35 correspondant on détecte que l'opération de sécurisation 34 n'a pas été réussie, le circuit 7 délivre un signal de rejet transmis par le connecteur 13 à l'interface 3. Dans ce cas le terminal 1 produit sur l'écran 3 un message indiquant l'échec.

La sécurisation peut par exemple concerner la vérification de ce qu'un code secret frappé sur le clavier 2 par un utilisateur correspond à un code secret mémorisé dans le circuit 22 de la carte 5.

Par contre si l'opération 34 a été réussie, alors on décide, selon l'invention, en une opération 36 d'augmenter le contenu du compteur 16. Après l'incrément 36 du compteur 16, le programme 32 aboutit à l'opération 31 comme auparavant.

Sur la figure 2, en ce qui concerne les opérations 28, 33 et 36 on a montré une duplication de ces opérations. Ceci est à mettre en rapport avec l'existence d'un autre compteur: le compteur 17. Selon l'invention on prévoit en effet de classer les demandes de transactions, selon leur nature, en plusieurs

classes. Il peut y avoir par exemple la classe des authentications, la classe des cryptages, la classe des déchiffrages de cryptogramme (lecture de certificat) et ainsi de suite. On crée alors autant de compteurs 16, 17 qu'il y a de classes gérées par les tests 28. On attribue de préférence à chaque classe un compteur différent. Ici on a montré deux classes correspondant aux compteurs 16 et 17. Autrement dit le test 28 cherchera à savoir si la transaction 25 demandée est une transaction correspondante à une instruction 29 ou si elle est par ailleurs une transaction correspondant à une autre instruction 37 du programme 30. Le compteur 16 compte le nombre de fois où l'instruction 29 est utilisée, le compteur 17 compte le nombre de fois où l'instruction 37 est utilisée. La classe est différenciée dans l'attribut.

On a préféré effectuer l'incrément du compteur après la vérification 35 de ce que l'opération 34 de sécurisation avait été réussie de manière à ne pas comptabiliser inutilement des opérations dans le circuit de sécurité 7 mis en place dans le lecteur 1 si un opérateur se trompe au cours de l'opération 34 en composant son numéro de code avec le clavier 2. La position de l'opération 36 dans l'arborescence issue de l'opération 33 peut néanmoins être quelconque, par exemple situé entre l'étape 33 et l'étape 34. Selon ce qui vient d'être dit de préférence elle est située à la fin de cette arborescence.

Les valeurs des compteurs 16 ou 17 ne sont pas inférieures à la valeur fixée lorsqu'ils ont atteint, en une transaction précédente, cette valeur fixée. Dans ce cas, en une opération 38 correspondant à un sous programme 39 mémorisé dans la mémoire 15 on provoque la ré-initialisation du compteur 16 ou 17 concerné. Cette

opération de ré-initialisation n'a rien de différent, dans l'invention, des formes qu'elle peut par ailleurs avoir d'une manière connue dans l'état de la technique. Le sous programme 39 pourra comporter notamment une  
5 procédure sécurisée, en particulier des vérifications de codes secrets comme cela va être expliqué ci-après.

Ces programmes 30, 32 et 39 peuvent être compris dans un programme principal unique. La représentation qui en est donnée ici est indiquée pour bien montrer  
10 l'apport de l'invention. Dans l'état de la technique seul existait le programme 30. Dans l'invention il existe en plus le programme 32 pour la mise en oeuvre des nouvelles opérations 33 et 36 et le programme 39 pour effectuer l'opération 38.

15 A titre d'exemple, une opération d'authentification entre un terminal 1 et une carte 5 est montrée sur la figure 4. Dans celle-ci, le terminal 1 envoie un aléa, une chaîne de caractères, toujours différente d'une session à une autre, à la carte à puce 5. La carte 5  
20 reçoit dans son circuit 22 la valeur de cet aléa. La carte 5 possède des moyens, notamment généralement un micro-processeur du même type que les micro-processeurs 11 et 18, et par ailleurs des indications secrètes, un code secret. Le micro-processeur de la carte est  
25 capable de mettre en oeuvre un algorithme de chiffrement pour chiffrer l'aléa en fonction de la valeur du code secret. Ce chiffrement résulte en un aléa crypté produit par la carte. La carte transmet alors l'aléa crypté de son connecteur à l'interface 21  
30 du terminal 1. Le terminal 1 est capable d'effectuer un cryptage de l'aléa (il le connaît puisque c'est lui qui l'a produit) par un numéro d'identification personnel (PIN: Personal Identification Number) frappé au clavier par l'utilisateur. Ce dernier cryptage résulte en un

PIN crypté. Le terminal 1 provoque alors la comparaison de l'aléa crypté au PIN crypté. Si la comparaison est positive, la suite de la transaction se produit sinon le terminal 1 en provoque le rejet.

5 Ces opérations ainsi montrées sous la référence 40 sont typiquement des opérations sensibles effectuées par le circuit de sécurité 7 à l'intérieur du terminal 1.

10 D'une manière comparable on peut prévoir qu'une combinaison de touches du clavier 2 conduise à une opération 38 de ré-initialisation du ou des compteurs 16 ou 17. Cette opération 38 comportera dans ce but une demande, affichée sur l'écran 3 du terminal 1 faite à l'opérateur de composer un numéro secret de ré-  
15 initialisation. Ce numéro secret ne sera pas un numéro PIN mais quelque chose d'équivalent. Une fois ce numéro secret composé, et une touche validation du clavier 2 enfoncée, le circuit 7 effectuera la comparaison, directe dans ce cas, du numéro secret composé avec un  
20 numéro attendu mémorisé dans sa mémoire 50. Si la comparaison est positive le compteur sélectionné est ré-initialisé. Il est disponible pour un même nombre de transactions.

25 De préférence, on effectue la ré-initialisation à distance par un système maître, par exemple à la suite d'une opération de collecte des données des transactions quotidiennes.

30 Pour empêcher que le fraudeur ne se serve d'un lecteur 1 pour tenter, frauduleusement, de réactiver le circuit 7, on pourra prévoir dans l'opération 38, un autre compteur du circuit 7, par exemple limité à trois opérations, au delà desquelles le circuit 7 sera définitivement neutralisé si le numéro secret composé est faux trois fois de suite. Ce comptage jusqu'à trois

peut être effectué par le terminal 1 (dans son programme 26) , il est de préférence effectué par le circuit 7 lui-même. En variante, le circuit 7 est à usage unique, dès que le compteur 16 ou 17 est bloqué, 5 il faut le remplacer par un nouveau circuit 7. Le cas échéant, on engage automatiquement une procédure d'effacement du contenu du SAM, en particulier, secrets et algorithmes de chiffrement.

En agissant ainsi on se rend compte qu'un fraudeur 10 n'aura qu'un nombre limité d'accès au circuit de sécurité 7. Au delà, le circuit 7 neutralisera tous les lecteur 1 dans lesquels il sera introduit.

Dans un exemple une action sensible est donc une authentification d'un porteur de la carte à puce. Dans 15 un autre exemple, une opération sensible peut tout simplement être un cryptogramme de certaines données, une procédure d'authentification réciproque. Des données sont ainsi transmises au circuit de sécurité 7 qui les restitue sous une forme cryptée, utilisable en 20 vue de leur transmission, ou de leur stockage dans la carte à puce 5. Dans le domaine du porte-monnaie électronique, il est prévu que la carte à puce comporte un état du solde du porte-monnaie et un certificat. Le certificat est un cryptogramme représentatif de la 25 cohérence du solde du porte-monnaie avec une information relative à la carte, par exemple son numéro de série, et une information variable, par exemple un compteur d'opérations qui compte le nombre de fois où on s'est servi du porte-monnaie. L'opération de 30 vérification de cryptogramme, opération sensible, effectuée par le circuit sécurisé consiste à recalculer le certificat sur ces bases, et à vérifier que celui qui était enregistré dans la carte à puce porte-monnaie est le même.

Pour limiter les opérations, on peut déjà les empêcher complètement. C'est ce qui a été vu jusqu'ici. Néanmoins, et ceci est représenté schématiquement par la liaison 41 en tirets, figure 2, on peut accepter un

5 fonctionnement dégradé du terminal 1. Dans ce fonctionnement dégradé, bien entendu aucune opération sensible ne peut être effectuée. Par contre des opérations anodines, visualisation de solde de compte,

10 de série, numéro de compte en banque, nom et adresse du porteur) peuvent être autorisées. Dans ce cas le programme 26 pourra continuer à se dérouler selon ce qui a été prévu par son concepteur. En effet, le programme 26 représente une partie de l'application et

15 il est possible que certaines actions puissent être exécutées même si par ailleurs d'autres opérations sensibles n'ont pu être vérifiées. L'autre partie de l'application est contenue dans le programme 30.

## REVENDEICATIONS

1 - Procédé de gestion d'un terminal (1) sécurisé (7) utilisé pour des transactions avec des cartes à puce comportant les étapes suivantes

5 - on met une carte (5) à puce (22) en relation avec le terminal,

- on fait exécuter un programme (26) par le terminal, ce programme comportant des opérations (29) sensibles relatives à la sécurisation des transactions, caractérisé en ce que

10 - on compte (32,16) le nombre de fois où le terminal est sollicité pour exécuter des opérations sensibles, et

- on limite l'action de ce terminal dès que ce compte atteint (33) une valeur fixée.

15 2 - Procédé selon la revendication 1, caractérisé en ce que

- on munit le terminal d'un circuit (8) électronique amovible de sécurité, et

20 - on compte (16) dans ce circuit le nombre d'opérations sensibles sollicitées auprès de lui ou exécutées par lui.

3 - Procédé selon l'une des revendications 1 à 2, caractérisé en ce que

25 - on répartit les opérations sensibles en plusieurs classes et

- on établit un compte (16,17) pour chaque classe.

4 - Procédé selon l'une des revendications 1 à 3, caractérisé en ce que

- comme opération sensible on exécute une procédure d'identification réciproque entre le terminal et la carte.

5 - Procédé selon l'une des revendications 1 à 4, caractérisé en ce que

- comme opération sensible on effectue une authentification (PIN) d'un porteur de la carte à puce.

6 - Procédé selon l'une des revendications 1 à 5, caractérisé en ce que

10 - comme opération sensible on effectue une vérification d'un certificat provenant d'une carte à puce.

7 - Procédé selon l'une des revendications 1 à 6, caractérisé en ce que

15 - on ré-initialise le compteur par une procédure sécurisée comportant une vérification d'un code secret par le terminal ou le circuit de sécurité.

8 - Procédé selon la revendication 7, caractérisé en ce que

20 - la procédure sécurisée comporte une vérification d'un code secret par le terminal ou le circuit de sécurité.

9 - Procédé selon la revendication 7, caractérisé en ce que

25 - la ré-initialisation est effectuée à distance par un système maître.

10 - Procédé selon l'une des revendications 1 à 9, caractérisé en ce que

30 - on incrémente le compteur après une opération sensible réussie.

11 - Procédé selon l'une des revendications 1 à 10, caractérisé en ce que

- pour limiter, on interdit une partie (47) seulement des opérations de la transaction projetée.

12 - Circuit de sécurité pour la mise en oeuvre du procédé selon l'une quelconque des revendications 1 à 5 11, caractérisé en ce qu'il comporte des moyens de gestion (16, 17, 32, 39) aptes à:

- identifier et comptabiliser des sollicitations provenant de l'extérieur et à limiter ses fonctions dès que la comptabilisation atteint un nombre prédéterminé.

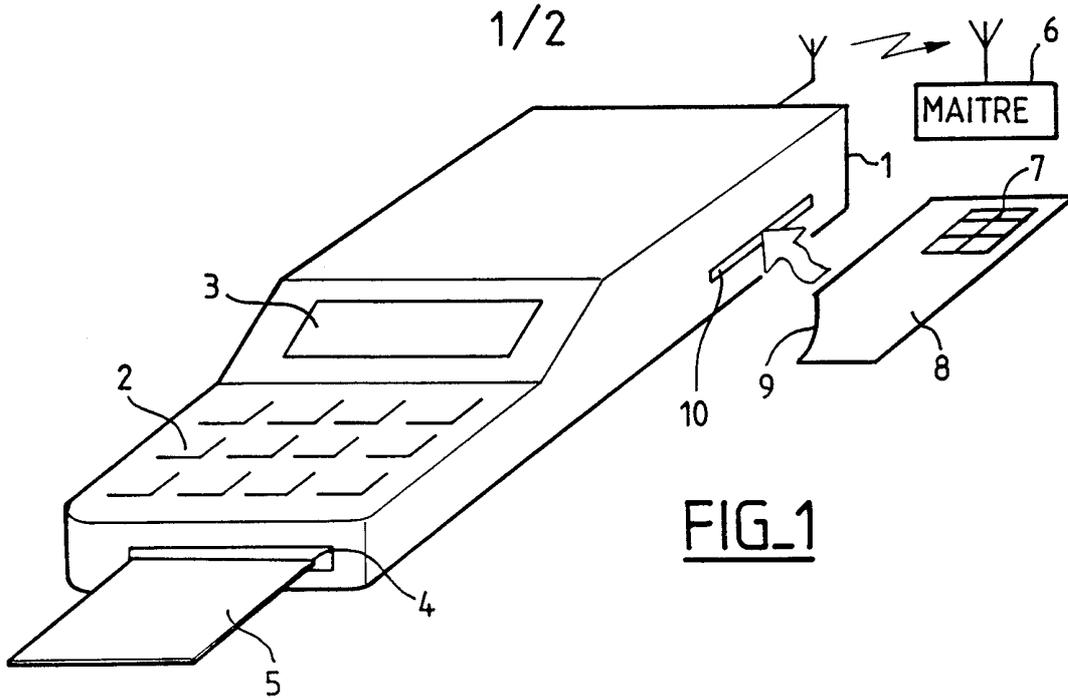


FIG. 1

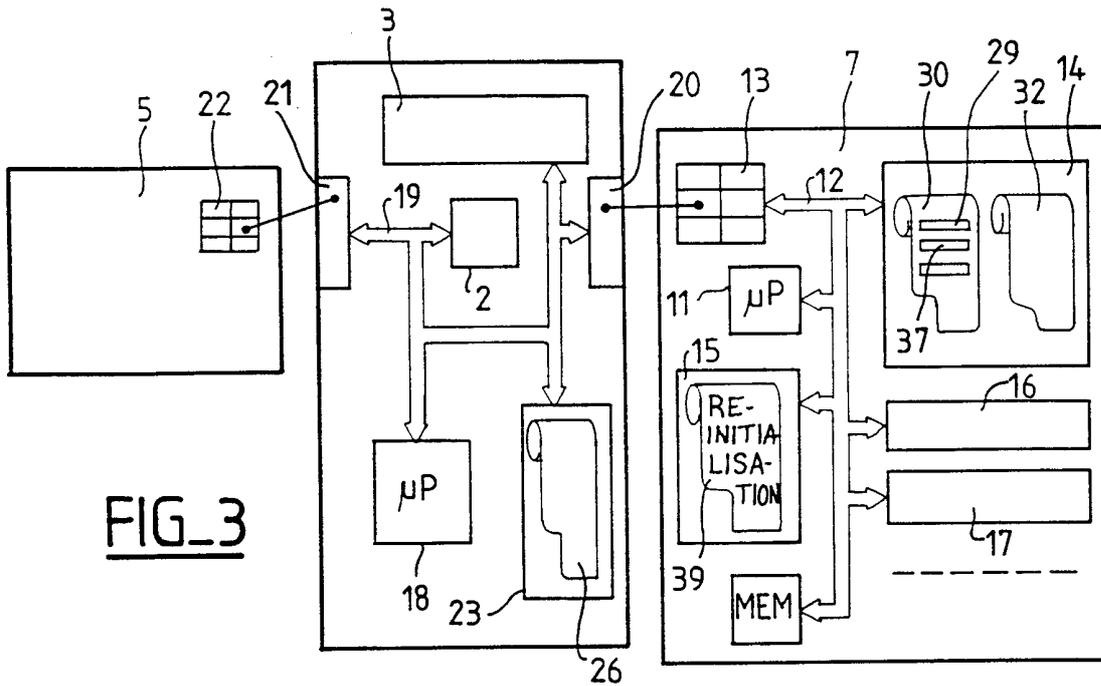


FIG. 3

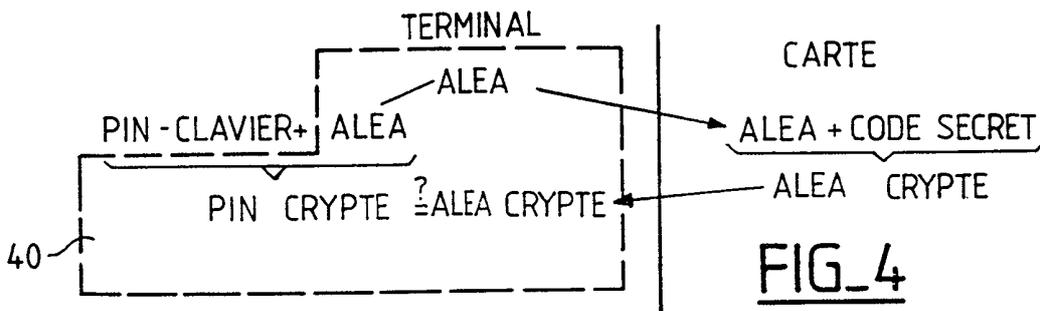
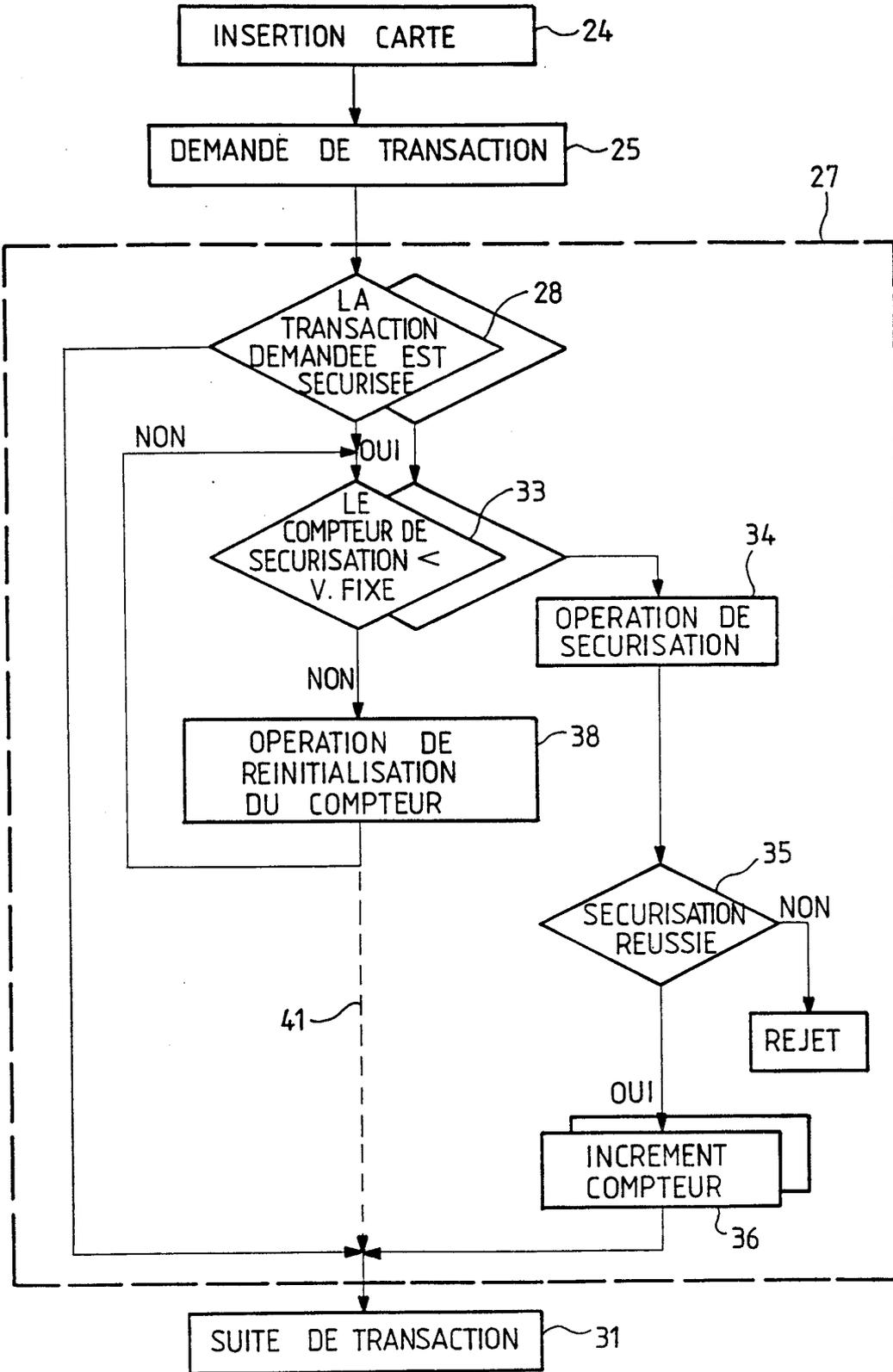


FIG. 4

2/2

FIG\_2



# INTERNATIONAL SEARCH REPORT

Inter: Application No
PCT/FR 98/01464

**A. CLASSIFICATION OF SUBJECT MATTER**  
 IPC 6 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)  
 IPC 6 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 157 303 A (TOSHIBA) 9 October 1985	1, 2, 10, 12
A	see abstract; claims; figures 1-4 see page 4, line 8 - page 5, line 25	3
Y	FR 2 674 647 A (M. WIDMER) 2 October 1992	1, 2, 10, 12
A	see abstract; claims; figures 1, 4, 5 see page 9, line 16 - page 11, line 22	5, 7, 8
A	EP 0 626 662 A (GEMPLUS CARD INTERNATIONAL) 30 November 1994 see abstract; claims; figures	1, 2, 4, 12
A	EP 0 696 016 A (FUJITSU) 7 February 1996	

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

\* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

22 October 1998

Date of mailing of the international search report

19/11/1998

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
 NL - 2280 HV Rijswijk  
 Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
 Fax: (+31-70) 340-3016

Authorized officer

David, J

# INTERNATIONAL SEARCH REPORT

Information on patent family members

Interr      Application No

PCT/FR 98/01464

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 0157303	A	09-10-1985	JP 60207957 A US 4879645 A	19-10-1985 07-11-1989
FR 2674647	A	02-10-1992	NONE	
EP 0626662	A	30-11-1994	FR 2705810 A US 5550919 A	02-12-1994 27-08-1996
EP 0696016	A	07-02-1996	JP 8044805 A	16-02-1996

# RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No  
PCT/FR 98/01464

**A. CLASSEMENT DE L'OBJET DE LA DEMANDE**  
CIB 6 G07F/10

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

**B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE**

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 6 G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)

**C. DOCUMENTS CONSIDERES COMME PERTINENTS**

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	EP 0 157 303 A (TOSHIBA) 9 octobre 1985	1, 2, 10, 12
A	voir abrégé; revendications; figures 1-4 voir page 4, ligne 8 - page 5, ligne 25	3
Y	FR 2 674 647 A (M. WIDMER) 2 octobre 1992	1, 2, 10, 12
A	voir abrégé; revendications; figures 1, 4, 5 voir page 9, ligne 16 - page 11, ligne 22	5, 7, 8
A	EP 0 626 662 A (GEMPLUS CARD INTERNATIONAL) 30 novembre 1994 voir abrégé; revendications; figures	1, 2, 4, 12
A	EP 0 696 016 A (FUJITSU) 7 février 1996	

Voir la suite du cadre C pour la fin de la liste des documents

Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

22 octobre 1998

Date d'expédition du présent rapport de recherche internationale

19/11/1998

Nom et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl.  
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

David, J

# RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Dema nationale No

PCT/FR 98/01464

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0157303 A	09-10-1985	JP 60207957 A US 4879645 A	19-10-1985 07-11-1989
FR 2674647 A	02-10-1992	AUCUN	
EP 0626662 A	30-11-1994	FR 2705810 A US 5550919 A	02-12-1994 27-08-1996
EP 0696016 A	07-02-1996	JP 8044805 A	16-02-1996