(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
2 août 2001 (02.08.2001)

PCT

(10) Numéro de publication internationale
WO 01/55980 A1

(51) Classification internationale des brevets[7] : G07F 7/10

(21) Numéro de la demande internationale :
PCT/FR01/00165

(22) Date de dépôt international :
18 janvier 2001 (18.01.2001)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
00/00829 24 janvier 2000 (24.01.2000) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **GEMPLUS** [FR/FR]; Avenue du Pic de Bertagne, Parc d'Activités de Gemenos, F-13420 Gemenos (FR).

(72) Inventeurs; et

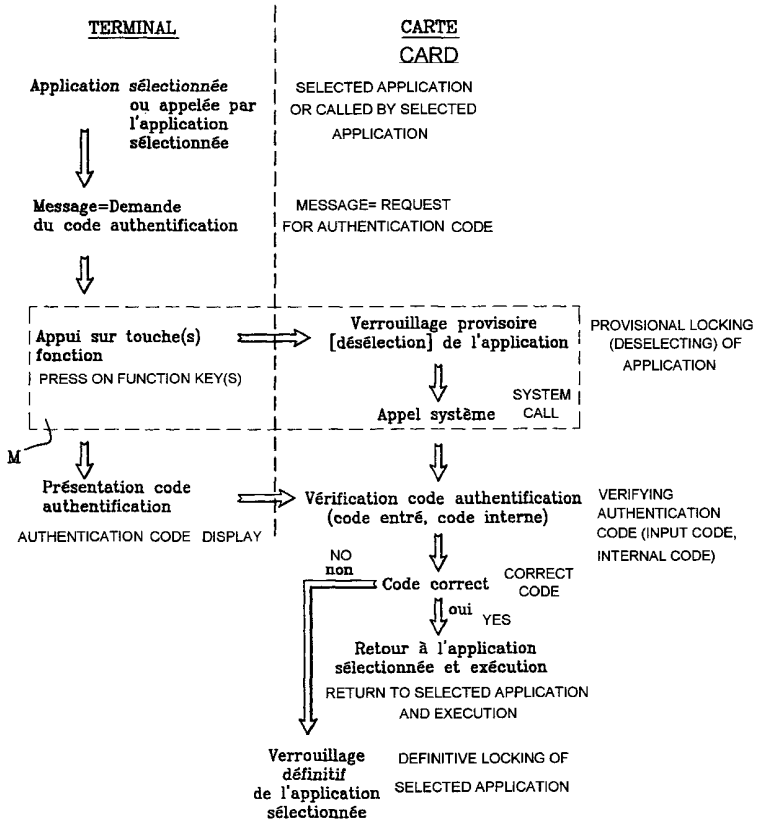
(75) Inventeurs/Déposants *(pour US seulement)* : **GIRARD, Pierre** [FR/FR]; 4, avenue Brue, F-13600 La Ciotat (FR). **BIDAN, Christophe** [FR/FR]; Rue du Moulin Neuf, F-35520 La Chapelle des Fougeretz (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS,

[Suite sur la page suivante]

(54) Title: METHOD FOR PROTECTING AGAINST THEFT THE AUTHENTICATING VALUE OF MULTIPLE APPLICATION SMART CARDS, SMART CARDS THEREFOR AND TERMINALS DESIGNED TO RECEIVE SAID CARDS

(54) Titre : PROCEDE DE PROTECTION CONTRE LE VOL DE LA VALEUR D'AUTHENTIFICATION POUR CARTES A PUCE(S) MULTI-APPLICATIONS, CARTES A PUCE(S) METTANT EN OEUVRE LE PROCEDE ET TERMINAUX SUSCEPTIBLES DE RECEVOIR LESDITES CARTES



(57) Abstract: The invention concerns a method for protecting against theft the authenticating value for multiple application smart cards. In order to prevent an application having access to a terminal from simulating the menu asking the user to present the authenticating value, the method provides a mechanism forcing access to the interface for presentation and verification of the authenticating value by the secure operating system whatever the application which has initiated the procedure, whenever there is a request for authenticating value. The invention is applicable to terminals (T) designed to communicate with smart cards (C) including therefor at least a function key (P_{IN}) or a sequence of function keys reserved for a system call to the card and to initiate presentation of the authenticating value.

[Suite sur la page suivante]

WO 01/55980 A1

LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) États désignés *(régional)* **:** brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, 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, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : L'invention concerne un procédé de protection contre le vol de la valeur d'authentification pour carte à puce(s) multi applications. Selon le procédé, il est prévu, pour empêcher une application possédant un accès vers un terminal de simuler le menu invitant l'utilisateur à présenter la valeur d'authentification, un mécanisme forçant l'accès à l'interface de présentation et de vérification de la valeur d'authentification par le système d'exploitation de la carte quelle que soit l'application ayant initié le processus, dès lors qu'il y a une demande de valeur d'authentification. L'invention s'applique à des terminaux (T) susceptibles de communiquer avec des cartes à puces (C) comprenant à cette fin au moins une touche fonction (P_{IN}) ou une séquence de touches fonction réservée pour effectuer un appel système à la carte et initier la présentation de la valeur d'authentification.

PROCEDE DE PROTECTION CONTRE LE VOL DE LA VALEUR D'AUTHENTIFICATION POUR CARTES A PUCE(S) MULTI-APPLICATIONS, CARTES A PUCE(S) METTANT EN ŒUVRE LE PROCEDE ET TERMINAUX SUSCEPTIBLES DE RECEVOIR LESDITES CARTES

L'invention concerne un procédé de protection contre le vol de la valeur d'authentification pour les cartes à puce(s) multi applications aptes à communiquer avec l'extérieur au moyen d'un terminal. Elle concerne également les cartes à puce(s) mettant en œuvre ledit procédé et les terminaux susceptibles de recevoir lesdites cartes. L'invention s'applique tout particulièrement aux cartes à puces multi applications utilisées avec les téléphones mobiles tels que les téléphones définis par le standard GSM.

On entend par cartes à puce(s) multi-applications des cartes contenant une ou plusieurs puces de circuit intégré lesdites cartes étant destinées à pouvoir exécuter différents programmes d'application chargés ou téléchargés au cours de la vie de la carte.

Parmi les solutions de cartes multi-applications existantes à ce jour, nous pouvons signaler « JavaCard » défini par Sun ou « SmartCard for Windows » défini par Microsoft.

Pour simplifier, on parlera dans la suite d'applications pour désigner les programmes d'applications (ou Applet en terminologie anglo saxonne).

On entend par valeur d'authentification, que l'on dénomme également code d'authentification, une valeur permettant d'authentifier le titulaire de la carte. La valeur d'authentification peut être une donnée connue

du titulaire seul (en général, un numéro d'identification personnel ou PIN- Personnal Identifier Number), déduite d'une caractéristique biométrique du titulaire (par exemple, voix, empreinte digitale, chaleur...) ou résultant d'une action que seul le titulaire peut effectuer (par exemple, signature).

Pour des raisons de compatibilité avec les cartes à puce(s) ne supportant qu'une unique application, et de simplicité pour l'utilisateur de la carte, les cartes à puce multi-applications ont généralement une seule valeur d'authentification pour toutes les applications. Ainsi, la spécification OP définie par VISA, et qui tient lieu actuellement de standard pour le chargement/téléchargement et la gestion interne d'applications sur les cartes à puce multi-applications, définit un unique PIN global pour toutes les applications résidentes et futures de la carte.

Le problème soulevé par le déposant dans le cas d'une carte multi-applications, vient de ce que la carte est prévue pour pouvoir charger ou télécharger de nouvelles applications pendant toute sa vie. A priori ceci est un avantage, mais en pratique cette caractéristique rend la carte vulnérable, car des applications malveillantes pourront être chargées avec d'autres applications de manière transparente vis à vis du titulaire. C'est donc une porte ouverte à de telles applications qui bien sûr en pratique vont chercher à découvrir la valeur d'authentification de la carte.

Suite à cette observation, le déposant a identifié une attaque permettant de trouver la valeur d'authentification de la carte.

Cette attaque suppose l'existence d'une application malveillante possédant un accès vers l'extérieur.

Une application possède un accès vers un terminal dès lors qu'il existe un terminal permettant à l'application de directement dialoguer avec l'utilisateur via ce terminal. On peut citer par exemple dans le cadre du GSM les applications pouvant modifier les menus affichés sur le téléphone mobile.

Voici alors la procédure suivie lors de cette attaque au moyen d'une application qui peut dialoguer avec l'extérieur.

En fait, l'application utilise sa capacité à dialoguer avec l'extérieur pour simuler sur le terminal l'interface qui permet de demander à l'utilisateur d'entrer la valeur d'authentification.

En effet, la vérification de l'identité de l'utilisateur de la carte est généralement réalisée par l'intermédiaire d'une application en charge d'afficher, sur l'écran du terminal dans lequel est insérée la carte à puce(s), un menu invitant l'utilisateur de présenter la valeur d'authentification. Une fois la valeur d'authentification présentée, le terminal retourne cette valeur à ladite application qui vérifie (éventuellement par l'intermédiaire d'une application en charge de la vérification de la valeur d'authentification) que la valeur présentée par l'utilisateur est identique à la valeur d'authentification de la carte. Si tel est le cas, l'application répond par l'affirmation ; par la négation dans le cas contraire.

L'accès à l'application en charge de l'affichage, sur l'écran du terminal dans lequel est insérée la carte à puce(s), du menu invitant l'utilisateur à présenter la valeur d'authentification est généralement contrôlée afin que seules les applications autorisées

puissent initier la vérification de la valeur d'authentification.

Néanmoins, une application malveillante possédant un accès vers un terminal peut simuler sur ce terminal le menu invitant l'utilisateur à présenter sa valeur d'authentification. L'utilisateur va alors en toute confiance présenter sa valeur d'authentification, permettant ainsi à l'application malveillante de découvrir cette valeur. Par la suite, l'application malveillante pourra, grâce à sa capacité de dialoguer vers l'extérieur, fournir la valeur d'authentification au développeur de l'application malveillante. Ceci sera d'autant plus facile dans le cas d'un terminal tel qu'un téléphone mobile pour lequel l'application malveillante pourra composer un numéro afin de communiquer la valeur d'authentification.

La présente invention a pour but de remédier à ces problèmes.

La présente invention a pour objet un procédé de protection contre le vol de la valeur d'authentification pour carte à puce(s) multi applications comprenant un système d'exploitation, principalement caractérisé en ce qu'il comprend, pour empêcher une application possédant un accès vers un terminal de simuler le menu invitant l'utilisateur à présenter la valeur d'authentification, un mécanisme forçant l'accès à l'interface de présentation de la valeur d'authentification par le système d'exploitation de la carte quelle que soit l'application ayant initié le processus, dès lors qu'il y a une demande de valeur d'authentification.

Selon une autre caractéristique, le mécanisme comporte la réservation sur le terminal d'au moins une touche fonction ou d'une séquence de touches fonction

apte à provoquer un appel du système d'exploitation de la carte.

La mise en œuvre du mécanisme comprend la séquence d'actions suivantes :

- l'appui sur la ou les touches fonction par l'utilisateur de la carte pour autoriser la présentation de la valeur d'authentification et provoquer un verrouillage provisoire des applications de la carte,
- la présentation de la valeur d'authentification,
- la mise en œuvre de la procédure de vérification de la valeur d'authentification par le système d'exploitation après les deux premières actions.

L'invention concerne également une carte à puce(s) multi applications comprenant un système d'exploitation et des moyens de communication avec un terminal, principalement caractérisé en ce qu'elle comprend des moyens pour que les appels système en provenance du terminal pour la présentation de la valeur d'authentification ne puissent être intercepter par les applications.

L'invention concerne un terminal susceptible de communiquer avec une carte à puce(s), principalement caractérisé en ce qu'il comprend au moins une touche fonction ou une séquence de touches fonction réservée pour effectuer un appel système à la carte et initier la présentation de la valeur d'authentification.

Le terminal pourra être un téléphone mobile par exemple du type GSM.

D'autres particularités et avantages de l'invention apparaîtront clairement à la lecture de la description qui est faite ci après et en regard des dessins sur lesquels :

- la figure 1 représente le schéma illustrant la mise en œuvre du procédé selon l'invention,
- la figure 2 représente le schéma d'un terminal susceptible de communiquer avec une carte à puce(s) selon l'invention,
- la figure 3 représente le schéma d'une carte multi application selon l'invention.

Une réalisation pratique du procédé selon l'invention va être décrite dans la suite en regard de la figure 1.

Le procédé comprend un verrouillage provisoire de l'application sélectionnée par l'utilisateur ou d'une application appelée par l'application sélectionnée par cet utilisateur ; un appel du système d'exploitation de la carte à puce(s) pour la mise en œuvre par le système d'exploitation de la procédure de vérification de la valeur d'authentification.

Selon la réalisation proposée, le verrouillage est obtenu par l'association d'une touche fonction ou d'une séquence de touches prévue sur le terminal pour pouvoir initier la présentation de la valeur d'authentification et un appel système déclenché par l'appui de cette touche fonction ou de la séquence de touches fonction. Dès lors que l'utilisateur voie apparaître un message de demande de la valeur d'authentification sur l'écran du terminal, il ne peut poursuivre la procédure de présentation de la valeur d'authentification qu'après avoir appuyé sur ladite touche, garantissant de cette manière que la procédure de vérification de la valeur d'authentification est effectuée par le système d'exploitation ou sous son contrôle.

En effet, lorsqu'une application s'exécute au sein de la carte et que le menu de présentation de la valeur d'authentification apparaît sur l'écran du terminal,

l'utilisateur doit appuyer sur la touche fonction prévue portant la référence P_{IN} sur les schémas (ou sur la séquence de touches fonction) pour présenter sa valeur d'authentification. Cette action permet de verrouiller provisoirement l'application en cours d'exécution (c'est à dire que l'application est suspendue) et de lancer un appel vers le système d'exploitation de la carte. C'est alors sous le contrôle du système d'exploitation qu'est effectuée la procédure de présentation et de vérification de la valeur d'authentification. Cette vérification consiste à comparer la valeur d'authentification présentée par l'utilisateur avec la valeur d'authentification mémorisée dans la carte.

Lorsque la valeur d'authentification présentée par l'utilisateur est correcte, le système d'exploitation de la carte déverrouille l'application en cours d'exécution qui peut alors reprendre son exécution à l'endroit où elle a été suspendue ; dans le cas contraire, le système d'exploitation affiche un message d'erreur et exécute les actions de sécurité adéquates (par exemple verrouiller définitivement l'application et afficher un message d'alerte).

La figure 2 illustre un terminal T apte à communiquer avec une carte à puce(s). Ce terminal possède de manière connue une unité centrale de traitement UC avec une mémoire de programme MPT. Cette mémoire comporte une interface IT de communication avec les cartes à puce(s) classique en soi. Seule une modification est prévue pour permettre au terminal de se mettre en attente de l'appui sur la touche P_{IN} (ou la séquence de touches fonction) après l'affichage du message de demande de la valeur d'authentification et

d'envoyer un appel au système d'exploitation de la carte.

Une carte à puce(s) C multi applications a été schématisée sur la figure 3 afin d'illustrer les différents éléments entrant dans la mise en œuvre du procédé conforme à l'invention. Prenons le cas pour simplifier où une seule puce P de circuit intégré est présente dans la carte, il s'agit d'une puce contenant un ou plusieurs microprocesseur(s) et ses mémoires associées en particulier une mémoire de programmes MPC. Cette mémoire contient le système d'exploitation et l'interface de présentation et de vérification de la valeur d'authentification. En général une autre mémoire de programmes MPA est destinée à mémoriser les différents programmes d'applications A1, A2,... An.

REVENDICATIONS

1.Procédé de protection contre le vol de la valeur d'authentification pour carte à puce(s) multi applications comportant un système d'exploitation et une interface de présentation et de vérification de la valeur d'authentification de l'utilisateur de ladite carte, caractérisé en ce qu'il comprend, pour empêcher une application possédant un accès vers un terminal de simuler le menu invitant l'utilisateur à présenter la valeur d'authentification, un mécanisme forçant l'accès à l'interface de présentation et de vérification de la valeur d'authentification par le système d'exploitation de la carte quelle que soit l'application ayant initié le processus, dès lors qu'il y a une demande de valeur d'authentification.

2. Procédé de protection contre le vol de la valeur d'authentification selon la revendication 1, caractérisé en ce que le mécanisme comporte la réservation sur le terminal d'au moins une touche fonction ou d'une séquence de plusieurs touches fonction apte à provoquer un appel du système d'exploitation de la carte.

3. Procédé de protection contre le vol de la valeur d'authentification selon la revendication 1 ou 2, caractérisé en ce que la mise en œuvre du mécanisme comprend la séquence d'actions suivantes :

- l'appui sur la ou les touches fonction par l'utilisateur de la carte pour autoriser la présentation de la valeur d'authentification et provoquer un verrouillage provisoire de l'application,
- la présentation de la valeur d'authentification,

- la mise en œuvre de la procédure de vérification de la valeur d'authentification par le système d'exploitation après les deux premières actions.

4. Carte à puce(s) multi applications comprenant un système d'exploitation et des moyens de communication avec un terminal, caractérisé en ce qu'elle comprend des moyens (MPC) pour que les appels système en provenance du terminal (T) pour la présentation de la valeur d'authentification ne puissent être interceptés par les applications de la carte.

5. Terminal susceptible de communiquer avec une carte à puce(s), caractérisé en ce qu'il comprend au moins une touche fonction (P_{IN}) ou une séquence de touches fonction réservée pour effectuer un appel système à la carte et initier la présentation de la valeur d'authentification.

6. Terminal selon la revendication 5, caractérisé en ce qu'il est constitué par un téléphone mobile.

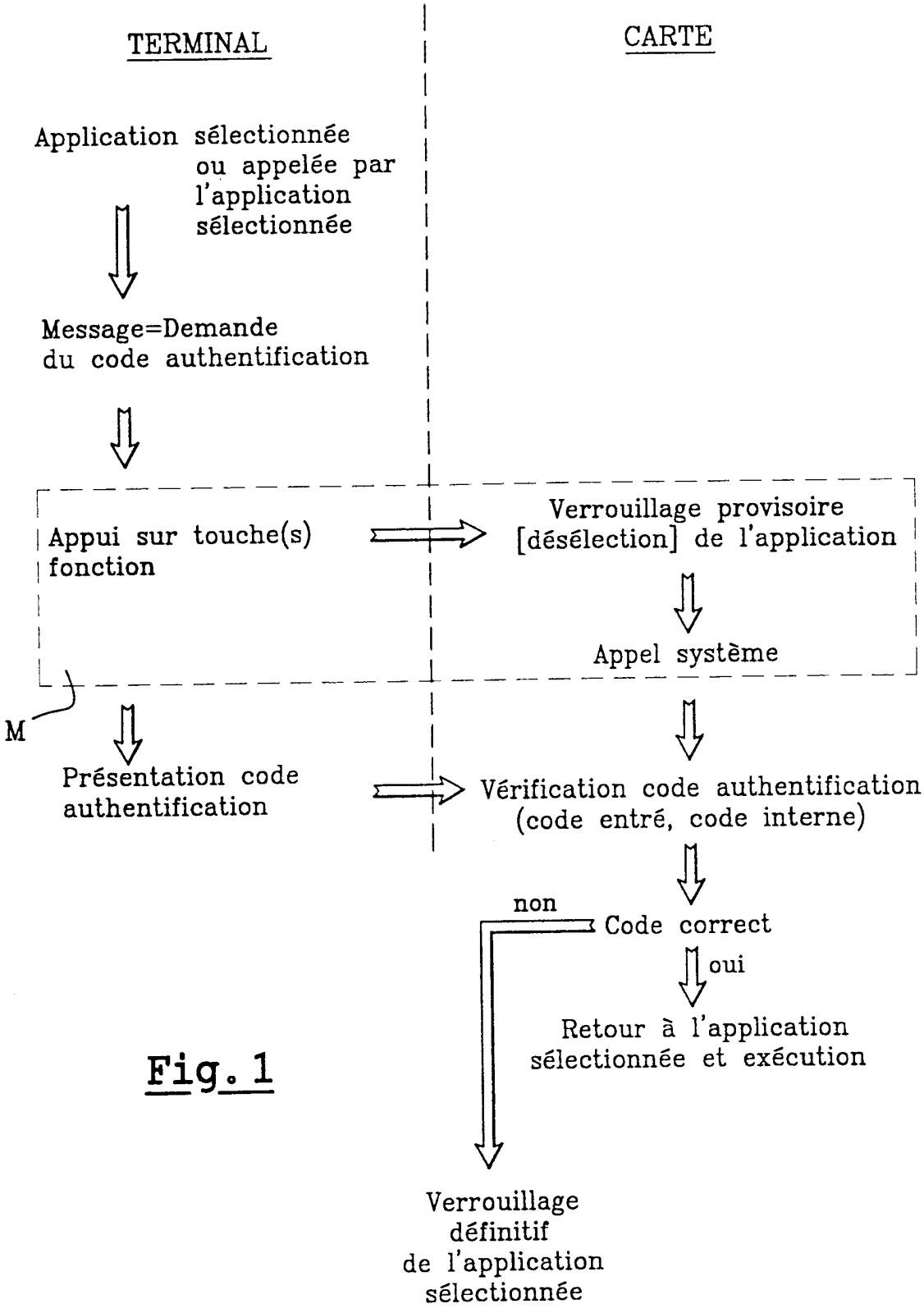

TERMINAL
CARTE
Application sélectionnée ou appelée par l'application sélectionnée
Message=Demande du code authentification
Appui sur touche(s) fonction
Verrouillage provisoire [désélection] de l'application
Appel système
M
Présentation code authentification
Vérification code authentification (code entré, code interne)
non
Code correct
oui
Retour à l'application sélectionnée et exécution
Verrouillage définitif de l'application sélectionnée

Fig. 1

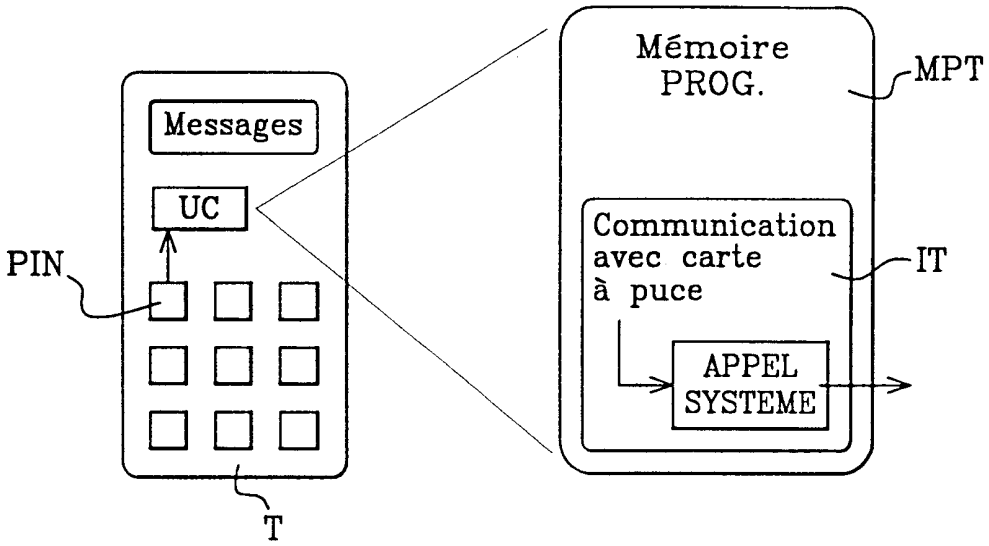

Mémoire
PROG.
MPT
Messages
UC
PIN
Communication
avec carte
à puce
IT
APPEL
SYSTEME
T

Fig. 2

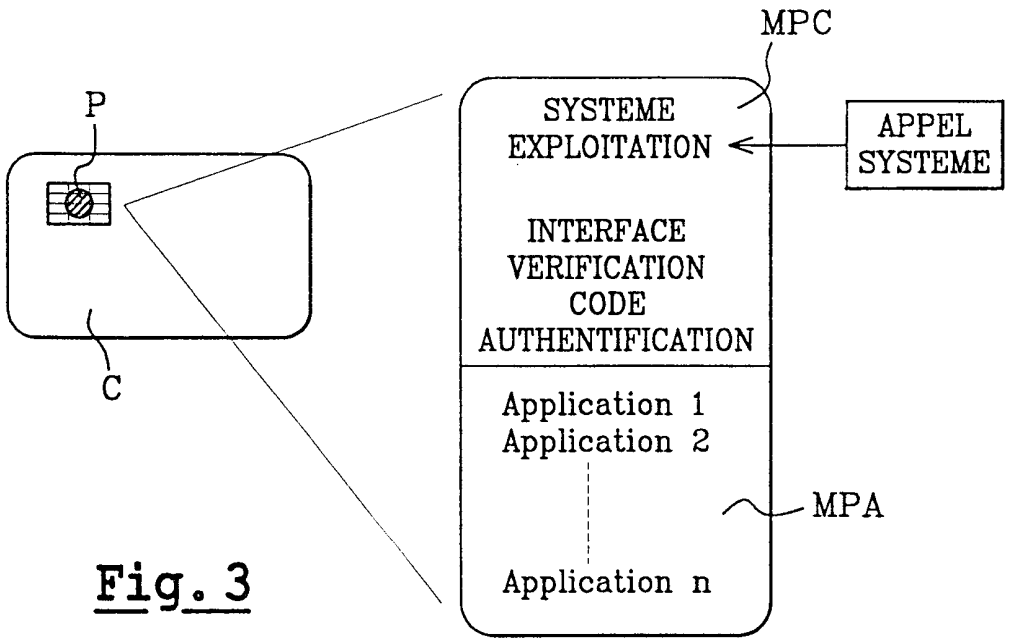

MPC
P
SYSTEME
EXPLOITATION
APPEL
SYSTEME
INTERFACE
VERIFICATION
CODE
AUTHENTIFICATION
Application 1
Application 2
MPA
Application n
C

Fig. 3

INTERNATIONAL SEARCH REPORT

Internatio Application No
PCT/FR 01/00165

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 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 7 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)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 325 776 A (IBM) 2 August 1989 (1989-08-02) page 3, line 5 - line 49	1-6
Y	US 6 005 942 A (CHAN ALFRED ET AL) 21 December 1999 (1999-12-21) column 3 -column 6	1-6

☐ 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	Date of mailing of the international search report
14 June 2001	22/06/2001

Name and mailing address of the ISA	Authorized officer
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	Wolles, B

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Internatio. ‹pplication No
PCT/FR 01/00165

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0325776 A	02-08-1989	US 4918653 A	17-04-1990
		DE 3851049 D	15-09-1994
		DE 3851049 T	09-03-1995
		JP 1233543 A	19-09-1989
US 6005942 A	21-12-1999	AU 6578698 A	20-10-1998
		EP 1004992 A	31-05-2000
		EP 1021801 A	26-07-2000
		US 6233683 B	15-05-2001
		WO 9843212 A	01-10-1998

RAPPORT DE RECHERCHE INTERNATIONALE

Demande ernationale No
PCT/FR 01/00165

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G07F7/10

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 consultee (systeme de classification suivi des symboles de classement)
CIB 7 G07F

Documentation consultee autre que la documentation minimale dans la mesure ou ces documents relevent des domaines sur lesquels a porte la recherche

Base de donnees electronique consultee au cours de la recherche internationale (nom de la base de donnees, et si realisable, termes de recherche utilises)
EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Categorie °	Identification des documents cites, avec, le cas echeant, l'indication des passages pertinents	no. des revendications visees
Y	EP 0 325 776 A (IBM) 2 août 1989 (1989-08-02) page 3, ligne 5 - ligne 49	1-6
Y	US 6 005 942 A (CHAN ALFRED ET AL) 21 décembre 1999 (1999-12-21) colonne 3 -colonne 6	1-6

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

☒ Les documents de familles de brevets sont indiqués en annexe

° Categories speciales de documents cités:

"A" document definissant l'etat général de la technique, non considere comme particulierement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou apres 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 a une divulgation orale, à un usage, à une exposition ou tous autres moyens

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

"T" document ultérieur publié apres la date de dépôt international ou la date de priorite et n'appartenenant pas a 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'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolement

"Y" document particulièrement pertinent; l'inven tion 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 a laquelle la recherche internationale a été effectivement achevée	Date d'expédition du present rapport de recherche internationale
14 juin 2001	22/06/2001

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
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	Wolles, B

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande .rnationale No
PCT/FR 01/00165

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0325776 A	02-08-1989	US 4918653 A	17-04-1990
		DE 3851049 D	15-09-1994
		DE 3851049 T	09-03-1995
		JP 1233543 A	19-09-1989
US 6005942 A	21-12-1999	AU 6578698 A	20-10-1998
		EP 1004992 A	31-05-2000
		EP 1021801 A	26-07-2000
		US 6233683 B	15-05-2001
		WO 9843212 A	01-10-1998