PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

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

(51) Classification internationale des brevets 6 : G07F 7/10, G06K 19/07	A1	(11) Numéro de publication internationale: **WO 96/38825** (43) Date de publication internationale: 5 décembre 1996 (05.12.96)

(21) Numéro de la demande internationale: PCT/FR96/00796

(22) Date de dépôt international: 28 mai 1996 (28.05.96)

(30) Données relatives à la priorité:
95/06370 30 mai 1995 (30.05.95) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: SYSECA S.A. [FR/FR]; 66-68, avenue Pierre-Brossolette, F-92240 Malakoff (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(US seulement)*: CESAIRE, Gérard [FR/FR]; (FR). DEVAUX, François [FR/FR]; (FR). GERARD, Yves [FR/FR]; Thomson-CSF SCPI, Boîte postale 329, F-92402 Courbevoie Cédex (FR).

(74) Mandataire: THOMSON-CSF SCPI; Boîte postale 329, F-92402 Courbevoie Cédex (FR).

(81) Etats désignés: CA, JP, US, brevet européen (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

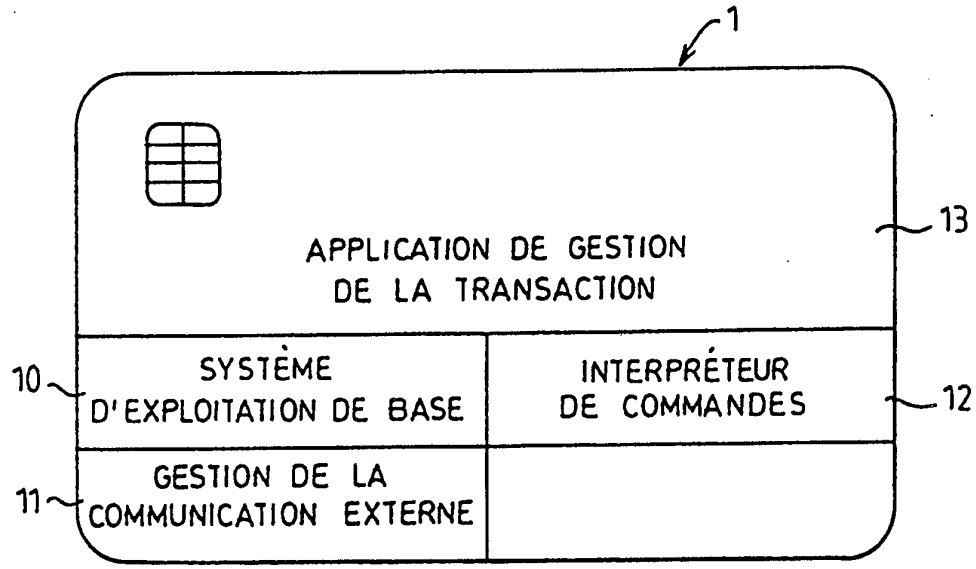
Publiée
Avec rapport de recherche internationale.
Avant l'expiration du délai prévu pour la modification des revendications, sera republiée si de telles modifications sont reçues.

(54) Title: PROTECTED SMART CARD

(54) Titre: CARTE A PUCE INTELLIGENTE SECURISEE

(57) Abstract

Smart cards are cards which control the execution of their own transactions, so as to avoid providing specialised card readers for each type of transaction. The protected smart card system (1) of the invention is a smart card storing a transaction management programme (13) written in a high-order language requiring interpretation by a command interpreter (12) through a basic operating system (10) with systems for protecting memory access. Hence, an unauthorised user cannot interfere with the integrity of a transaction, since he can only access the smart card through the high-order language, and the high-order language commands which he might divert would necessarily be intercepted by the command interpreter (12) and by the protection systems of the basic operating system (10).



(57) Abrégé

Les cartes à puce intelligentes sont celles qui contrôlent elles-mêmes le déroulement de leur transaction afin d'éviter de spécialiser un lecteur par type de transaction. La carte à puce intelligente sécurisée (1) concernée par l'invention est une carte à puce intelligente qui renferme stocké en mémoire un programme de gestion de transaction (13) écrit dans un langage évolué nécessitant une interprétation par un interpréteur de commandes (12) passant par un système d'exploitation de base (10) pourvu de systèmes de sécurisation des accès à la mémoire. Grâce à cela, un utilisateur non habilité ne peut porter atteinte à l'intégrité d'une transaction puisque qu'il n'a accès dans la carte à puce qu'au niveau du langage évolué et que les ordres de ce langage évolué qu'il pourrait détourner sont nécessairement interceptés par l'interpréteur de commande (12) et par les systèmes de sécurisation du système d'exploitation de base (10).

CARTE A PUCE INTELLIGENTE SECURISEE

On désigne par carte à puce, les cartes, en général du format d'une carte de crédit, mais également les jetons munis d'un microcircuit électronique, à base de mémoires et d'un microcontrôleur, agencées pour permettre le déroulement d'une transaction par exemple bancaire ou santé.

Les cartes à puce communiquent avec leur environnement au moyen de lecteurs équipés d'éléments de communication suffisant pour permettre et faciliter l'exécution de leur transaction.

Les cartes à puce actuellement connues, dotées de mémoires et éventuellement d'un microcontrôleur, sont utilisées uniquement comme un support de données agrémenté de dispositifs de sécurisation. L'intelligence nécessaire à la conduite des transactions est reportée au niveau des lecteurs qui sont soit autonomes et pourvus d'un clavier, d'un afficheur et d'une mémoire gérés par un microcontrôleur doté d'un programme de contrôle de déroulement de transaction spécifique à la transaction envisagée, soit transparents et utilisés comme accès à un système informatique programmé spécialement pour la transaction envisagée.

Ce report de l'intelligence nécessaire à la conduite d'une transaction, soit au niveau du lecteur de carte, soit à celui d'un système informatique associé au lecteur de carte, a pour inconvénient de nécessiter une spécialisation du lecteur ou du système informatique associé en fonction du type de transaction. Ainsi, si l'on veut changer de type de transaction, il ne suffit pas de changer la programmation de la carte à puce ; il faut aussi changer celle du lecteur, s'il est autonome, ou du système informatique associé, si le lecteur est transparent. Cela est un obstacle au développement des applications des cartes à puce.

Pour éviter cet inconvénient, il a été proposé de ramener l'intelligence, c'est à dire la gestion de la transaction, au niveau de la carte à puce elle-même. La carte à puce ne se contente plus d'effectuer les instructions qui lui parviennent de l'extérieur en les accompagnant d'éventuelles mesures de sécurité ; elle prend la maîtrise du déroulement de la transaction en donnant ses instructions au lecteur qui devient un simple exécutant et qui, de ce fait, peut être banalisé et utilisé avec des cartes à

puce de différentes sortes, spécialisées chacune dans des transactions très variées.

Il se pose alors des problèmes de capacité de mémoire carte si l'on veut stocker le programme de gestion de transaction dans la carte et de sécurisation si l'on veut éviter les opérations frauduleuses. Pour résoudre ces problèmes, il a été proposé dans la demande de brevet français FR-A-2 667 171 (GEMPLUS CARD INT.) et dans la demande internationale de brevet WO-A-94 10657 (INTELLECT AUSTRALIA) de passer pour le programme de gestion de la transaction par un langage de programmation intermédiaire qui nécessite un interpréteur dans la carte pour être assemblé et exécutable par le microprocesseur de la carte.

Si l'on obtient bien par ce procédé un gain de place en mémoire carte, on ne résout que partiellement le problème de la sécurisation. En effet, les interpréteurs proposés donnent un accès direct aux instructions en langage machine assurant la gestion de la mémoire carte si bien qu'il subsiste un risque de manipulation frauduleuse des données de la carte.

La présente invention a pour but d'améliorer la sécurité d'une carte à puce intelligente, tout en laissant la possibilité au promoteur d'une transaction de modifier cette transaction à loisir.

Elle a pour objet une carte à puce intelligente, sécurisée, équipée d'une mémoire dont une partie est permanente et d'un microcontrôleur, comportant, stocké en mémoire, un interpréteur de commandes assemblant, en un code exécutable par le microcontrôleur, des instructions d'un programme de gestion de transaction écrit en un langage évolué ineffectif sans traduction par l'interpréteur de commandes, remarquable en ce qu'elle comporte en outre un système d'exploitation de base assurant la gestion sécurisée des accès à la mémoire permanente avec des clefs d'autorisation pour certaines zones, et en ce que l'interpréteur de commandes passe par l'intermédiaire du système d'exploitation de base pour toutes les actions touchant à la mémoire permanente.

Avantageusement, le programme de gestion de transaction écrit en langage évolué est stocké dans un fichier, dans une partie réinscriptible de la mémoire permanente de type EEPROM.

Avantageusement, le système d'exploitation de base et l'interpréteur de commandes du langage interprété sont disposés dans une partie non réinscriptible de la mémoire permanente, de type ROM.

Le programme de gestion de transaction, lorsqu'il est stocké dans la carte à puce, communique avec le monde extérieur à la carte à puce et peut, par conséquent, être l'objet de tentatives de corruption. Le fait qu'il soit en langage évolué et interprété nécessitant, pour être exécuté par le microcontrôleur de la carte à puce, une traduction par un interpréteur de commandes s'appuyant, pour toute action sur la mémoire permanente, sur un système d'exploitation de base à sécurités d'accès permet de faire échec à de telles tentatives de corruption puisqu'il n'existe pas de possibilités accès direct entre l'interpréteur de commandes et la mémoire permanente. L'interpréteur de commandes et le système d'exploitation de base étant inaccessibles de l'extérieur de la carte à puce, grâce aux sécurités d'accès de la mémoire, sont eux, à l'abris des tentatives de corruption. En effet, le programme de gestion de la transaction peut accéder en lecture ou en écriture aux données stockées dans la partie EEPROM de la mémoire mais toujours sous contrôle du système d'exploitation de base qui vérifie le respect des sécurités accès à la mémoire.

Le langage évolué et interprété a également l'avantage de permettre d'écrire des programmes plus compacts qu'un langage non interprété de sorte qu'il économise de l'espace mémoire.

D'autres caractéristiques et avantages de l'invention ressortiront de la description ci-après d'un mode de réalisation de l'invention donné à titre d'exemple. Cette description sera faite ci-après en regard du dessin dans lequel :

- une figure 1 est un schéma de principe du microcircuit électronique équipant une carte à puce,
- une figure 2 illustre, de manière schématique, les différentes couches logiques du programme d'un microcontrôleur de carte à puce intelligente sécurisée selon l'invention, et
- une figure 3 est un schéma de principe de l'organisation de la mémoire d'une carte à puce.

On distingue sur la figure 1 le microcircuit électronique ou puce d'une carte à puce. Celui-ci comporte un microcontrôleur (CPU) 2 en liaison

avec de la mémoire vive (RAM) 3, de la mémoire permanente, morte non réinscriptible (ROM) 4 et réinscriptible (EEPROM) 5 et un port série d'entrées/sorties 6 menant à un ensemble de six à huit contacts électriques 7 permettant d'accéder à un lecteur.

La figure 2 montre les grandes partitions des programmes de gestion du microcontrôleur d'une carte à puce intelligente selon l'invention. La couche la plus enfouie est un système d'exploitation de base 10, en code exécutable adapté au type de microcontrôleur de la carte à puce 1, qui gère sa mémoire avec, pour la partie permanente de la mémoire, les systèmes habituels de sécurisation et un protocole de communication externe 11. Ce système d'exploitation de base 10 est associé à un interpréteur de commandes 12 auquel il passe la main dès qu'il reçoit une instruction d'exécution. L'interpréteur de commandes 12 est capable de reconnaître différentes instructions en langage évolué et repasse la main au système d'exploitation de base 10 dès que possible et, dans tous les cas, chaque fois qu'il s'agit de réaliser une action sur la mémoire permanente de la carte à puce. L'ensemble du système d'exploitation de base 10 et de l'interpréteur de commande 12 réside en mémoire morte non réinscriptible ROM et est surmonté par une couche externe constituée par un programme 13, en langage évolué et interprété, de gestion de la transaction à laquelle est dédiée la carte à puce, qui est stocké en mémoire morte réinscriptible EEPROM.

Le programme de gestion de transaction 13 communique avec l'extérieur de la carte à puce par l'intermédiaire du système d'exploitation de base. Par sécurité, toutes les instructions qu'il contient, notamment celles qui ont une action sur la mémoire permanente : lecture, écriture, effaçage, sont en langage évolué. De ce fait, elles sont incomprises du microcontrôleur si elles n'ont pas été interprétées par l'interpréteur de commande 12, qui les traduit et les dirige obligatoirement vers le système d'exploitation de base 10 et ses systèmes de sécurisation pour toute action sur la mémoire permanent de la carte. Vis à vis des actions sur la mémoire permanente de la carte, le programme de gestion de transaction, une fois assemblé par l'interpréteur de commandes 12, se comporte envers le système d'exploitation de base comme le port de communication externe SIO 6. De la sorte, toute action sur la mémoire permanente de la carte est

régie par les mêmes règles qu'elle ait pour origine une commande en provenance du port de communication externe ou du programme de gestion de transaction mémorisé dans la carte. Ainsi, un utilisateur non habilité, ne peut porter atteinte à l'intégrité d'une transaction puisqu'il n'a accès dans la carte à puce qu'au niveau du langage évolué et interprété, et que les ordres de ce langage évolué et interprété qu'il pourrait détourner sont nécessairement interceptés par les systèmes de sécurisation du système d'exploitation de base 10 dès qu'ils ont trait à la mémoire permanente de la carte.

L'utilisation d'un langage évolué devant être interprété, au niveau des échanges de la carte à puce avec l'extérieur, présente, également l'avantage, outre la sécurité qu'il apporte, de permettre d'écrire des programmes plus compacts et par conséquent d'économiser de l'espace mémoire.

La mémoire, qui est constituée des parties vive (RAM) 3, et mortes non réinscriptible (ROM) 4 et réinscriptible (EEPROM) 5, a sa partie morte réinscriptible (EEPROM) 5 organisée, comme le montre la figure 2, selon une arborescence de répertoires dont les accès sont réglementés en fonction de leurs niveaux au moyen de serrures qui doivent être ouvertes au préalable à l'aide de clefs constituées par des codes. Le répertoire racine 20 est dit maître. Il donne accès à un ou plusieurs niveaux inférieurs de répertoires 21, 22 dits répertoires dédiés. Les répertoires maître et dédiés renferment des fichiers élémentaires 200, 210, 220 et 221.

Le répertoire maître 20 est pourvu d'une protection de premier rang et renferme dans ses fichiers élémentaires un programme maître de gestion de transaction. Le gestionnaire du répertoire maître peut transmettre des droits à divers promoteurs d'application de rangs inférieurs enregistrés aux niveaux des répertoires dédiés et leur proposer en menu les applications qu'il autorise.

Le répertoire dédié 21 est pourvu d'une protection de deuxième rang et destiné à un promoteur d'applications de deuxième rang qui n'a pas généralement accès au répertoire maître mais qui peut créer, dans son répertoire, des applications en langage évolué avec droits d'accès.

Le répertoire dédié 22 est pourvu d'une protection de troisième rang et destiné à un promoteur d'application de troisième rang et ainsi de suite.

Grâce à cette hiérarchisation des répertoires et de leurs clefs d'accès, on peut faire cohabiter des applications gérées par des promoteurs d'application différents et indépendants. Chaque application étant installée dans un répertoire dédié à accès protégé par une clef spécifique, un utilisateur ne peut toucher à l'intégrité des données de la carte que dans les répertoires dont il possède les clefs accès. Même lorsqu'il est dûment autorisé à modifier une application, l'utilisateur ne peut agir sur la mémoire permanente de la carte sans passer par les sécurités d'accès du système d'exploitation de base car l'application pour avoir un effet sur la carte doit être écrite dans le langage évolué et interprété qui fait systématiquement appel aux sécurités d'accès du système d'exploitation de base pour toute opération sur la mémoire permanente de la carte.

Pour la réalisation d'une transaction, la carte à puce intelligente sécurisée communique en langage évolué et interprété, par l'intermédiaire du système d'exploitation de base, avec un lecteur qui lui fournit les ressources nécessaires telles que clavier, afficheur, liaison avec une ou plusieurs autres cartes à puce ou avec un système informatique. Cette communication se fait, à l'alternat, sur l'initiative du lecteur qui est électriquement maître des échanges mais sous le contrôle logique de la carte à puce qui définit les étapes successives d'une transaction par le déroulement de son programme de gestion de transaction.

Le lecteur a la maîtrise électrique des échanges grâce à deux commandes qu'il émet en alternance à destination de la carte à puce, d'une part, une requête de mise à disposition d'un paquet d'instructions et de données élaborées au sein de la carte à puce dit "message carte" et d'autre part, une déclaration de compte rendu associée à un message de compte rendu sur l'exécution d'instructions reçues précédemment dans des messages carte. Ces deux commandes sont avantageusement la commande "get response" et la commande "enveloppe" ou "execute" définies dans les normes ISO 7816/prEN726.

La commande "get response" est constituée par l'envoi d'un message binaire comprenant cinq champs successifs de un octet :

- un premier champ nommé "CLA" renfermant un octet identifiant la classe de l'instruction, par exemple, instructions réservées aux applications bancaires,

- un deuxième champ nommé "INS" renfermant l'octet C0 en hexadécimal identifiant le type de commande, "get response",

- un troisième champ réservé nommé "P1" renfermant l'octet 00 en hexadécimal,

- un quatrième champ réservé nommé "P2" renfermant l'octet 00 en hexadécimal, et

- un cinquième champ nommé "Le field" renfermant un octet dont la valeur n correspond au nombre d'octets attendus en réponse de la carte à puce.

Cette commande "get response" entraîne une réponse de la carte à puce dite "Data field" renfermant n octets de données, n étant le nombre déclaré dans son champ "Le field", et deux octets "SW1, SW2" de compte rendu carte.

La commande "execute" est constituée par l'envoi d'un message binaire constitué de cinq champs successifs de un octet et d'un champ final de données de plusieurs octets:

- un premier champ nommé "CLA" renfermant un octet identifiant la classe de l'instruction, par exemple, instructions réservées aux applications bancaires,

- un deuxième champ nommé "INS" renfermant l'octet AE en hexadécimal identifiant le type de commande "execute",

- un troisième champ réservé nommé "P1" renfermant l'octet 00 en hexadécimal,

- un quatrième champ réservé nommé "P2" renfermant l'octet 00 en hexadécimal,

- un cinquième champ nommé "Lc field" renfermant un octet dont la valeur n correspond au nombre d'octets du message accompagnant la commande "execute", et

- un sixième champ final nommé "Data field" renfermant les n octets de données annoncés dans le cinquième champ "Lc field". Cette commande "execute" entraîne une réponse de la carte à puce de deux octets "SW1, SW2" donnant un compte rendu carte.

La commande "enveloppe" a la même constitution que la commande "execute" et s'en différencie par la valeur de l'octet de son deuxième champ "INS" identifiant la commande qui vaut C2 en hexadécimal.

Dans ces trois messages, les champs respectifs "Le field" et "Lc field" déclarent la longueur du message carte attendu ou celle du message compte rendu du lecteur au moyen desquels transitent les instructions à exécuter et données associées en provenance de la carte à puce ainsi qu'en retour les comptes-rendus des actions exécutées par le lecteur et données résultantes.

A l'introduction de la carte à puce intelligente dans le lecteur, la carte à puce se trouve détectée et mise sous tension par le lecteur qui lui envoie un ordre de remise à zéro selon la norme ISO 7816-3. Il en résulte un processus d'initialisation du microcontrôleur de la carte à puce intelligente qui se termine par l'envoi au lecteur, depuis la carte à puce intelligente, d'une réponse d'acquittement à l'ordre de remise à zéro et par une mise en route du programme de gestion de transaction de la carte à puce intelligente pour un premier cycle de traitement aboutissant dans cette dernière à la préparation du premier message carte qui sera communiqué au lecteur dès que celui-ci en fera la demande au travers d'une requête de mise à disposition de message sous la forme d'une commande "get response".

A la réception de la réponse d'acquittement à l'ordre de remise à zéro, le lecteur entame un premier cycle d'échange de données avec la carte à puce intelligente.

Au cours de ce premier cycle d'échange, le lecteur envoie en direction de la carte à puce intelligente une requête de mise à disposition de message, sous la forme d'une commande "get response", pour demander l'envoi du message carte préparé par la carte à puce intelligente après son initialisation.

La carte à puce intelligente, à la réception d'une telle requête par la commande "get response", envoie le message carte préparé au lecteur.

Le lecteur reçoit le message carte, identifie les données qu'il contient, interprète le message, exécute les commandes demandées et répond à la carte à puce intelligente par une déclaration de compte rendu sous la forme d'une commande "enveloppe" ou "execute", avec un message de compte rendu rapportant à la carte à puce intelligente la façon dont il a

réalisé ce qui lui a été demandé et le résultat de ce traitement. Cela termine le premier cycle d'échange.

A la réception de la commande "enveloppe" ou "execute" du premier cycle d'échange en provenance du lecteur, la carte à puce intelligente poursuit le déroulement de son programme de gestion de transaction au cours d'un deuxième cycle de traitement pendant lequel elle vérifie d'abord l'exécution correcte du message carte qu'elle vient d'émettre au moyen du message de compte rendu, puis prépare un autre message carte.

Le lecteur entame ensuite un deuxième cycle d'échange en envoyant à la carte à puce intelligente une deuxième commande "get response" pour lire le nouveau message carte. Après traitement des données de ce nouveau message carte, le lecteur rend compte de son exécution à la carte à puce intelligente, au moyen d'un message de compte rendu incorporé à une deuxième commande "enveloppe" ou "execute" qui clôt le deuxième cycle d'échange.

La carte à puce intelligente, à la réception de cette deuxième commande "enveloppe" ou "execute" en provenance du lecteur entame alors, toujours sous le contrôle de son programme de gestion de transaction, un troisième cycle de traitement au cours duquel elle vérifie l'exécution correcte du message carte qu'elle vient d'émettre, au moyen du message de compte rendu reçu du lecteur, puis prépare un autre message carte.

Le lecteur entame alors un troisième cycle d'échange en envoyant à la carte à puce intelligente une troisième commande "get response" pour recevoir ce message carte.

Les cycles de traitement, à l'initiative de la carte à puce intelligente, et d'échange, à l'initiative du lecteur, se succèdent en fonction du programme de gestion de la transaction stocké dans la carte à puce intelligente.

Conformément à la norme ISO 7816-3 le lecteur 1 est électriquement maître des échanges, mais le déroulement de la transaction se fait à l'initiative de la carte à puce 4 qui est intelligente.

Le lecteur peut comporter plusieurs connecteurs de carte à puce. Dans ce cas, une seule carte à puce intelligente à la fois pilote la transaction. La carte à puce intelligente qui pilote la transaction est dite

"active". Les autres sont dites "passives". La carte à puce intelligente déclarée active est la première qui est capable de fournir une réponse a une instruction "get response" du lecteur.

REVENDICATIONS

1. Carte à puce intelligente sécurisée (1), équipée d'une mémoire (3, 4, 5) dont une partie (4,5) est permanente et d'un microcontrôleur (2), comportant, stocké en mémoire, un interpréteur de commandes (12) assemblant en un code exécutable par le microcontrôleur (2), des instructions d'un programme de gestion de transaction écrit en un langage évolué ineffectif sans traduction par l'interpréteur de commandes (12), caractérisée en ce qu'elle comporte en outre un système d'exploitation de base (10) assurant la gestion sécurisée des accès à la mémoire permanente (4, 5) avec des clefs d'autorisation pour certaines zones, et en ce que l'interpréteur de commandes (12) passe par l'intermédiaire du système d'exploitation de base (10) pour toutes les actions touchant à la mémoire permanente (4,5).

2. Carte à puce intelligente sécurisée selon la revendication 1, caractérisée en ce qu'elle comporte en mémoire permanente (5) au moins un fichier (200, 210, 211) contenant un programme de gestion de transaction en langage évolué et interprété.

3. Carte à puce intelligente sécurisée selon la revendication 2, caractérisée en ce que ledit fichier contenant un programme de gestion de transaction (13) en langage évolué et interprété est stocké en une zone de la mémoire permanente qui est morte et réinscriptible de type EEPROM.

4. Carte à puce intelligente sécurisée selon la revendication 1, caractérisée en ce que ledit système d'exploitation de base (10) et ledit interpréteur de commandes (12) sont stockés en une zone de la mémoire permanente qui est morte et non réinscriptible de type ROM.

5. Carte à puce intelligente sécurisée selon la revendication 1, caractérisée en ce qu'elle comporte en outre des moyens de communication (6) capable de communiquer à l'alternat et en langage évolué et interprété avec un lecteur sous le contrôle du système d'exploitation de base (10), chaque communication étant laissée à l'initiative du lecteur qui est

électriquement maître des échanges mais restant sous le contrôle logique de la carte à puce.

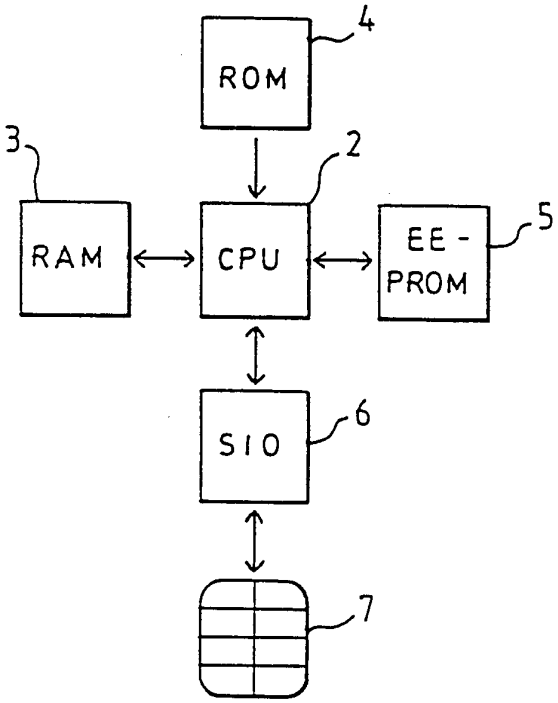

ROM
4
3
2
RAM
CPU
EE - PROM
5
SIO
6
7

FIG.1

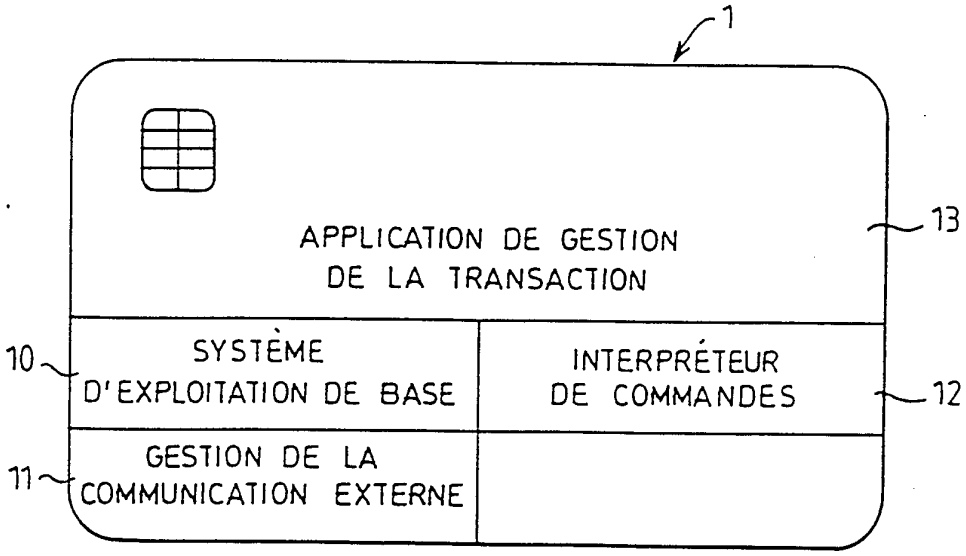

1
APPLICATION DE GESTION DE LA TRANSACTION
13
10
SYSTÈME D'EXPLOITATION DE BASE
INTERPRÉTEUR DE COMMANDES
12
11
GESTION DE LA COMMUNICATION EXTERNE

FIG.2

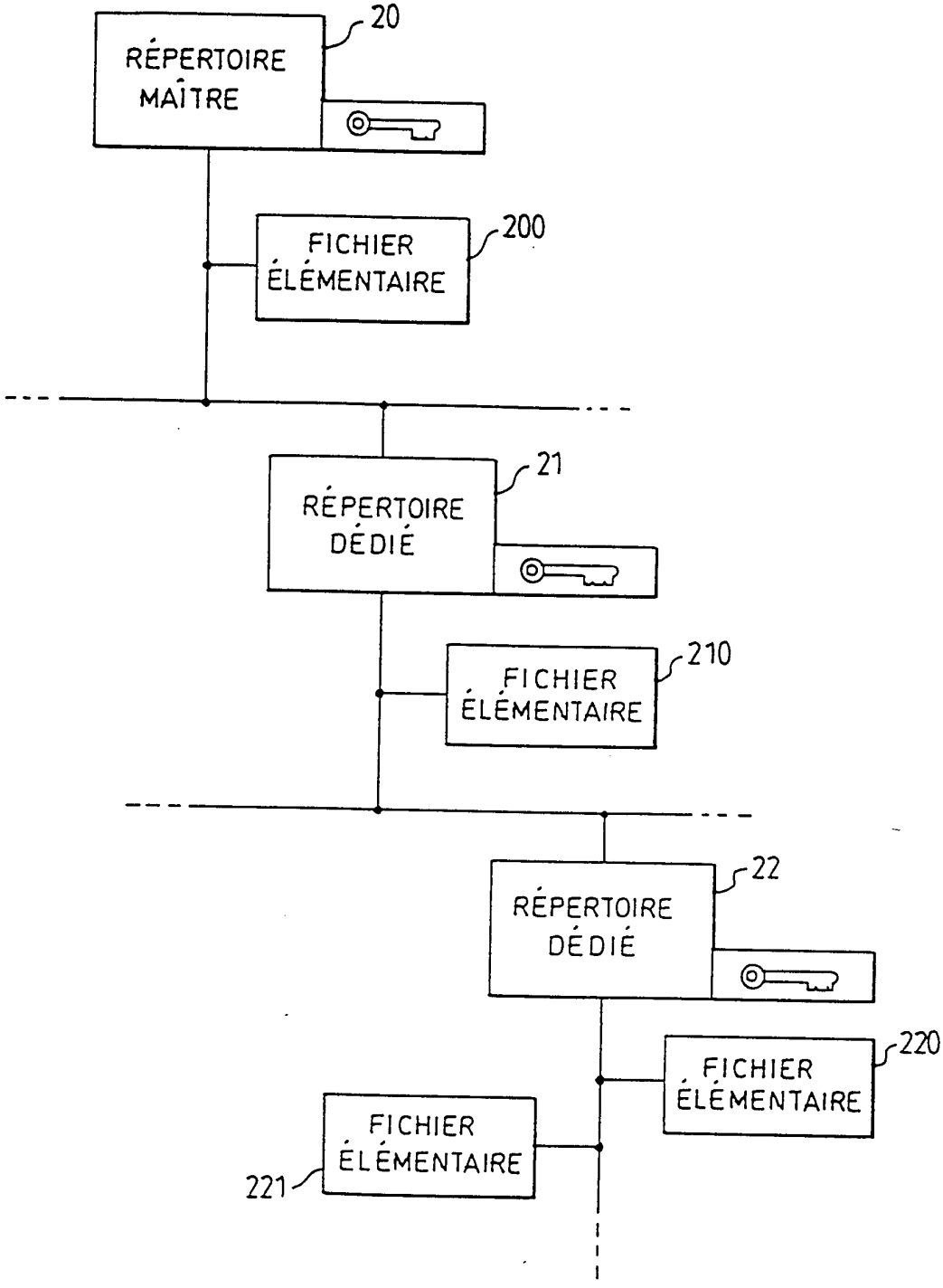

RÉPERTOIRE MAÎTRE
20
FICHIER ÉLÉMENTAIRE
200
RÉPERTOIRE DÉDIÉ
21
FICHIER ÉLÉMENTAIRE
210
RÉPERTOIRE DÉDIÉ
22
FICHIER ÉLÉMENTAIRE
220
FICHIER ÉLÉMENTAIRE
221

FIG. 3

INTERNATIONAL SEARCH REPORT

national Application No
PCT/FR 96/00796

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/10 G06K19/07

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 G06K G06F

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 A	FR,A,2 667 171 (GEMPLUS CARD INTERNATIONAL) 27 March 1992 cited in the application see abstract; claims 1-5; figures 1-3	1 3-5
Y A	EP,A,0 368 752 (BULL CP8) 16 May 1990 see abstract; claims; figures 1-4 see column 5, line 38 - column 6, line 17	1 2
A	WO,A,94 10657 (INTELLECT AUSTRALIA) 11 May 1994 cited in the application see abstract; claims 1-31; figures 1-9 see page 19, paragraph 2 - page 37, paragraph 1	1,3-5
A	FR,A,2 657 445 (GEMPLUS CARD INTERNATIONAL) 26 July 1991	

☐ 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

1

Date of the actual completion of the international search	Date of mailing of the international search report
17 October 1996	15. 11. 96

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	David, J

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

national Application No
PCT/FR 96/00796

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
FR-A-2667171	27-03-92	NONE		
EP-A-0368752	16-05-90	FR-A-	2638868	11-05-90
		CA-A-	2002349	09-05-90
		WO-A-	9005347	17-05-90
		JP-B-	7048178	24-05-95
		JP-T-	3500827	21-02-91
		US-A-	5434999	18-07-95
WO-A-9410657	11-05-94	AU-A-	5332194	24-05-94
		CA-A-	2147824	11-05-94
		EP-A-	0706692	17-04-96
		NO-A-	951575	26-06-95
FR-A-2657445	26-07-91	EP-A-	0446081	11-09-91
		JP-A-	4213116	04-08-92
		US-A-	5212369	18-05-93

RAPPORT DE RECHERCHE INTERNATIONALE

ande Internationale No
PCT/FR 96/00796

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 G07F7/10 G06K19/07

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 G06K G06F

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	FR,A,2 667 171 (GEMPLUS CARD INTERNATIONAL) 27 Mars 1992 cité dans la demande	1
A	voir abrégé; revendications 1-5; figures 1-3	3-5

Y	EP,A,0 368 752 (BULL CP8) 16 Mai 1990	1
A	voir abrégé; revendications; figures 1-4 voir colonne 5, ligne 38 - colonne 6, ligne 17	2

A	WO,A,94 10657 (INTELLECT AUSTRALIA) 11 Mai 1994 cité dans la demande voir abrégé; revendications 1-31; figures 1-9 voir page 19, alinéa 2 - page 37, alinéa 1	1,3-5

	-/--	

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

[X] 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'appartenenant 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

1

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
17 Octobre 1996	15. 11. 96

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	David, J

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

:ande Internationale No
PCT/FR 96/00796

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	FR,A,2 657 445 (GEMPLUS CARD INTERNATIONAL) 26 Juillet 1991	

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

ande Internationale No
PCT/FR 96/00796

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
FR-A-2667171	27-03-92	AUCUN		
EP-A-0368752	16-05-90	FR-A-	2638868	11-05-90
		CA-A-	2002349	09-05-90
		WO-A-	9005347	17-05-90
		JP-B-	7048178	24-05-95
		JP-T-	3500827	21-02-91
		US-A-	5434999	18-07-95
WO-A-9410657	11-05-94	AU-A-	5332194	24-05-94
		CA-A-	2147824	11-05-94
		EP-A-	0706692	17-04-96
		NO-A-	951575	26-06-95
FR-A-2657445	26-07-91	EP-A-	0446081	11-09-91
		JP-A-	4213116	04-08-92
		US-A-	5212369	18-05-93