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 19/073

A1

(11) Numéro de publication internationale: WO 97/14121

(43) Date de publication internationale: 17 avril 1997 (17.04.97)

(21) Numéro de la demande internationale: PCT/FR96/01583

(22) Date de dépôt international: 11 octobre 1996 (11.10.96)

(30) Données relatives à la priorité:
95/12183 11 octobre 1995 (11.10.95) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: GEMPLUS [FR/FR]; Avenue du Pic-de-Bertagne, Parc d'Activités de Gémenos, Boîte postale 100, F-13881 Gémenos Cédex (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(US seulement)*: CUNIN, Hervé [FR/FR]; Chemin de Banon N, La Petite Arcadie, F-13100 Aix-en-Provence (FR). LAFFONT, Eric [FR/FR]; Le Balzac Bâtiment A, 2ème étage, Allée de Callelongue, F-13008 Marseille (FR). ODDOU, Wilfrid [FR/FR]; Océanie 3, La Baie des Anges, F-13600 La Ciotat (FR).

(74) Mandataire: NONNENMACHER, Bernard; Gemplus S.C.A., Z.I. Athelia III, Voie Antiope, F-13705 La Ciotat (FR).

(81) Etats désignés: AL, AM, AU, BB, BG, BR, CA, CN, CZ, EE, FI, GE, HU, IS, JP, KG, KP, KR, KZ, LK, LR, LT, LV, MD, MG, MK, MN, MX, NO, NZ, PL, RO, SG, SI, SK, TR, TT, UA, US, UZ, VN, brevet ARIPO (KE, LS, MW, SD, SZ, UG), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

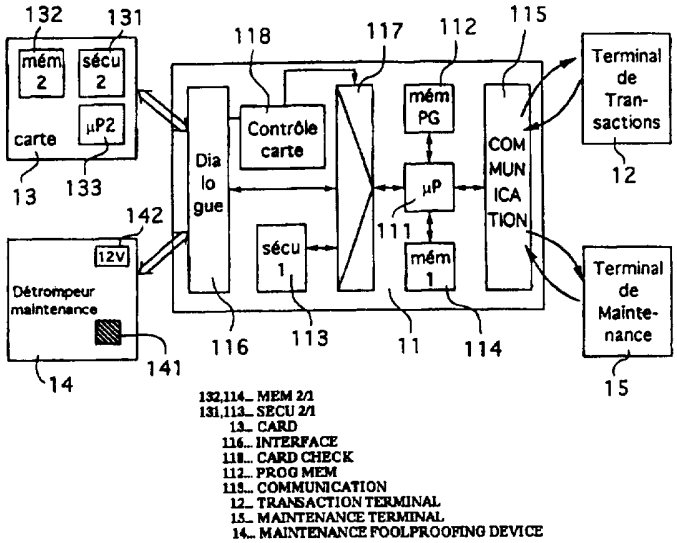
Publiée
Avec rapport de recherche internationale.
Avant l'expiration du délai prévu pour la modification des revendications, sera republiée si de telles modifications sont reçues.

(54) Title: PORTABLE DEVICE FOR PERFORMING SECURE INTERNAL AND SMART CARD TRANSACTIONS, AND METHOD THEREFOR

(54) Titre: DISPOSITIF PORTATIF DESTINE A EFFECTUER DES TRANSACTIONS SECURISEES EN INTERNE ET PAR CARTE A MICRO-CIRCUITS, ET PROCEDE DE MISE EN OEUVRE CORRESPONDANT

(57) Abstract

A portable device (11) for performing secure transactions with transaction terminals (12), including first means (111, 113) for performing a secure transaction using first transaction resources stored in a first memory (114), and means (115) for contactless communication with said transaction terminals. The device includes means (116) for interfacing with a smart card (13) including second means (131, 133) for performing a secure transaction, and means (117) for selecting one of the first secure transaction means and the second secure transaction means, with particular reference to data on the presence and validity of said card, whereby a transaction may be performed either by the portable device (11) or by said smart card (13). In either case, data communication with said transaction terminals (12) is provided by said contactless communication means (115).



(57) Abrégé

L'invention concerne un dispositif portatif (11) destiné à effectuer des transactions sécurisées avec des terminaux de transaction (12), comprenant des premiers moyens (111, 113) permettant la réalisation d'une transaction sécurisée, à partir de premières ressources de transactions stockées dans une première mémoire (114), et des moyens (115) de communication sans contact avec lesdits terminaux de transaction. Selon l'invention, le dispositif comprend des moyens (116) de dialogue avec une carte (13) à micro-circuits comprenant des seconds moyens (131, 133) permettant la réalisation d'une transaction sécurisée, et des moyens (117) de sélection entre lesdits premiers moyens de transaction sécurisée et lesdits seconds moyens de transaction sécurisée, tenant compte notamment d'informations représentatives de la présence et de la validité de ladite carte, de façon qu'une transaction puisse être réalisée soit par ledit dispositif portatif (11), soit par ladite carte à micro-circuits (13), l'échange de données avec lesdits terminaux de transaction (12) étant dans les deux cas assuré par lesdits moyens (115) de communication sans conctact.

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.

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

Dispositif portatif destiné à effectuer des transactions sécurisées en interne et par carte à micro-circuits, et procédé de mise en oeuvre correspondant.

Le domaine de l'invention est celui des transactions électroniques sans contact, notamment dans le domaine du paiement électronique. Plus précisément, l'invention concerne une amélioration des dispositifs permettant d'effectuer de telles transactions.

Le paiement dit électronique est une technique bien connue. Son aspect le plus commun est celui des cartes à micro-circuits, qui sont désormais très répandues. On peut distinguer deux grands types de cartes : les cartes de crédit, qui correspondent essentiellement à une authentification du porteur, autorisant un débit sur un compte bancaire, et les cartes prépayées, qui portent un montant débité au fur et à mesure des opérations. Ces dernières cartes sont avantageusement rechargeables.

Un inconvénient majeur des cartes utilisées actuellement est qu'elle doivent être introduites dans des terminaux prévus à cet effet, afin de lire les informations qu'elles contiennent. Cette opération est contraignante, et parfois peu aisée, pour l'utilisateur, et entraîne une détérioration des éléments de contact de la carte, du fait des frottements successifs.

Afin de pallier cet inconvénient, on a imaginé des dispositifs similaires aux cartes à micro-circuits classiques, mais capables de dialoguer à distance (sans contact) avec des terminaux.

Toutefois, ces dispositifs sans contact ne sont pas encore disponibles sur le marché, alors que de nombreux types de cartes sont utilisés depuis longtemps. La diffusion de tels dispositifs s'avère donc difficile, car ils doivent cohabiter avec les cartes déjà distribuées. Cela pose des problèmes d'une part pour l'usager, qui doit connaître les deux procédures d'utilisation, et d'autre part pour les terminaux, qui doivent être équipés de lecteurs de cartes et de moyens de communication sans contact.

L'invention a notamment pour objectif de pallier ces inconvénients de l'état de la technique.

Plus précisément, un objectif de l'invention est de fournir un dispositif de transactions sans contact qui puisse être introduit sans imposer la suppression

systématique des cartes déjà mises en oeuvre pour la même application.

Un autre objectif de l'invention est de fournir une technique permettant de réaliser des terminaux simples, ne prévoyant qu'un seul type de moyens de dialogue avec les objets de transaction.

Un objectif de l'invention est également de fournir un tel dispositif, qui soit simple et convivial d'utilisation, et qui offre de nombreuses facilités, telles que la consultation ou la configuration.

Encore un autre objectif de l'invention est de permettre une plus grande facilité d'utilisation des cartes à micro-circuits de types connus, tant pour les opérations de paiement que pour les opérations de rechargement.

L'invention a également pour objectif de fournir un dispositif de transaction sans contact dont la mise à jour (configuration, maintenance, ...) soit aisée et ne nécessite pas de moyens spécifiques importants, notamment à l'intérieur du dispositif, tant pour des raisons d'encombrement que de coût de revient.

Ces objectifs, ainsi que d'autres qui apparaîtront par la suite, sont atteints selon l'invention à l'aide d'un dispositif portatif destiné à effectuer des transactions sécurisées avec des terminaux de transaction, comprenant des premiers moyens permettant la réalisation d'une transaction sécurisée, à partir de premières ressources de transaction stockées dans une première mémoire, et des moyens de communication sans contact avec lesdits terminaux de transaction, et comprenant de plus des moyens de dialogue avec une carte à micro-circuits comprenant des seconds moyens permettant la réalisation d'une transaction sécurisée, et des moyens de sélection entre lesdits premiers moyens de transaction sécurisée et lesdits seconds moyens de transaction sécurisée, tenant compte notamment d'informations représentatives de la présence et de la validité de ladite carte, de façon qu'une transaction puisse être réalisée soit par ledit dispositif portatif, soit par ladite carte à micro-circuits, l'échange de données avec lesdits terminaux de transaction étant dans les deux cas assuré par lesdits moyens de communication sans contact.

Par transaction, on entend dans la présente demande toute opération nécessitant un échange d'information entre le dispositif ou la carte et un terminal. Dans le cadre des systèmes de paiement, il peut notamment s'agir de paiements (similaires à l'émission de

chèques), de rechargements (retraits de chèques et/ou en monnaie) ou de dépôts (de chèques et/ou de monnaie).

L'invention concerne donc un produit totalement nouveau, qui permet d'utiliser de la même façon les dispositifs de transaction sans contact et les cartes à micro-circuits déjà développées. Ainsi, l'utilisation des cartes est grandement améliorée, puisqu'elles acquièrent la qualité des dispositifs sans contact, et la diffusion des dispositifs est facilitée, puisqu'ils permettent l'utilisation des cartes pré-existantes et la réalisation de terminaux ne comprenant que des moyens de communication sans contact.

Cette technique n'est nullement évidente pour l'homme du métier, car elle réunit deux types d'objet qu'il a l'habitude de considérer comme indépendants et concurrents. Selon l'invention, le dispositif sans contact n'est pas le remplaçant de la carte à micro-circuits, mais un élément coopérant avec celle-ci, afin de lui fournir la qualité de communication sans contact.

L'utilisation des mêmes moyens de communication permet bien sûr un gain appréciable.

Il est à noter que selon l'invention, le dispositif et la carte conservent leur indépendance, en matière de mise en oeuvre de la transaction. Toutes les opérations de sécurisation sont effectuées par l'élément en charge de la transaction. En d'autres termes, la carte n'est pas une simple mémoire venant alimenter le dispositif, mais un élément capable d'effectuer toutes les opérations de transaction.

Ainsi, la mise en oeuvre du dispositif selon l'invention prévoit deux modes de fonctionnement :

- un mode direct, dans lequel la transaction est gérée par ledit dispositif portatif ; et
- un mode transparent, dans lequel la transaction est gérée par une carte à micro-circuits couplée opérationnellement audit dispositif,

une communication sans contact avec lesdits terminaux de transaction étant mise en oeuvre de façon identique dans les deux modes.

Selon un mode réalisation préférentiel de l'invention, lesdits premiers moyens de transaction sécurisée et/ou lesdits seconds moyens de transaction sécurisée assurent

l'émission de chèques électroniques portant un montant transmis par un terminal de transaction, et authentifiés par une signature cryptée à l'aide d'un algorithme à clé publique, lesdits chèques étant stockés sous forme vierge dans une mémoire réinscriptible.

D'autres techniques sont bien sûr envisageables. Notamment, la carte à micro-circuits peut être une carte de crédit bancaire, ce qui permet de regrouper les avantages des systèmes à pré-paiement (dans le dispositif) et des systèmes à crédit (dans la carte).

De façon avantageuse, le dispositif de l'invention comprend des moyens de rechargement en ressources de transaction dudit dispositif, par une communication sans contact avec un terminal de rechargement.

Dans ce cas notamment, le dispositif peut comprendre des moyens de transfert de ressources de transaction dudit dispositif vers une desdites cartes à microcircuits et/ou d'une desdites cartes à micro-circuits vers ledit dispositif. Cela permet en particulier de recharger une carte par une communication sans contact, par l'intermédiaire de la mémoire du dispositif.

Selon un mode de réalisation préférentiel de l'invention, lesdits moyens de dialogue peuvent recevoir un élément de contrôle de configuration et/ou de maintenance comprenant des moyens pour le distinguer d'une desdites cartes à micro-circuits, et autorisant la configuration et/ou la maintenance dudit dispositif à partir d'un terminal de contrôle, par l'intermédiaire desdits moyens de communication sans contact.

Ainsi, la réalisation technique du dispositif est simplifiée. En effet, tous les échanges de données utilisent les mêmes moyens de communication. La sécurité est cependant assurée par la présence d'un élément détrompeur : il n'est pas possible qu'une fausse manoeuvre (ou une manoeuvre frauduleuse) affecte la configuration du dispositif. Ce détrompeur étant reçu par les moyens de dialogue avec la carte, on réduit à nouveau la complexité de fabrication, et donc le coût de revient et l'encombrement du dispositif.

Selon un autre mode de réalisation, lesdits moyens de dialogue peuvent recevoir un élément de configuration et/ou de maintenance comprenant des moyens pour le distinguer d'une desdites cartes à micro-circuits, et assurant la configuration et/ou la maintenance dudit dispositif.

En d'autres termes, l'élément introduit dans les moyens de dialogue n'est plus un simple détrompeur, mais un élément intelligent, capable de prendre en charge la configuration ou la maintenance du dispositif.

De façon avantageuse, ledit élément de contrôle ou ledit élément de configuration et/ou de maintenance délivre une tension électrique supérieure à la tension électrique de fonctionnement dudit dispositif, et permettant d'effacer et de reprogrammer le contenu d'une mémoire reprogrammable.

Préférentiellement, lesdits moyens de communication sans contact sont des moyens de communication par infrarouge. De façon avantageuse, ladite communication sans contact est une communication du type maître-esclave, le terminal de transaction jouant le rôle du maître et ledit dispositif jouant le rôle de l'esclave.

Selon un mode de réalisation avantageux de l'invention, lesdits moyens de dialogue avec une carte à micro-circuits fonctionnent à une fréquence de transmission nominale prédéterminée, et comprennent des moyens de détection de défauts de transmission, entraînant le passage à une fréquence de transmission de repli correspondant à la moitié de ladite fréquence de transmission nominale.

La fréquence de repli peut notamment être la fréquence normalisée 3,5 MHz, la fréquence nominale étant alors 7 MHz.

Dans un mode de réalisation particulier de l'invention, le dispositif comprend un multiplexeur associant à un port unique d'accès à un microprocesseur de contrôle soit lesdits moyens de dialogue avec une carte à micro-circuits, soit des moyens de sécurisation interne d'une transaction.

Selon un mode de mise en oeuvre, on prévoit que ledit multiplexeur connecte systématiquement lesdits moyens de dialogue avec une carte à micro-circuits lorsque la présence d'une carte valide est détectée.

L'invention concerne également un procédé de mise en oeuvre du dispositif portatif décrit ci-dessus.

Ce procédé peut notamment mettre en oeuvre au moins une des opérations consistant à :

- assurer l'émission de chèques électroniques portant un montant transmis par un

terminal de transaction ;

- sécuriser un chèque par la transmission d'une signature cryptographique ;
- gérer au moins deux soldes correspondant à des devises différentes, de façon à permettre le paiement dans plusieurs devises et/ou à transcrire des montants transmis dans plusieurs devises ;
- assurer le dépôt et/ou le retrait d'un montant sur un compte ;
- valider l'utilisateur du dispositif et/ou de la carte à l'aide d'un code confidentiel ;
- recharger en chèques vierges et/ou en un montant financier ledit dispositif ;
- transférer des chèques (vierges ou crédités) et/ou un montant financier dudit dispositif vers une desdites cartes à micro-circuits et/ou d'une desdites cartes à micro-circuits vers ledit dispositif ;
- consulter un solde (montants et chèques) du dispositif et/ou de la carte, une liste des dernières transactions et/ou des taux de change ;
- configurer et personnaliser le fonctionnement du dispositif.

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

- la figure 1 est un schéma synoptique simplifié illustrant le principe général de l'invention ;
- la figure 2 illustre de façon plus détaillée un mode de réalisation particulier du dispositif de la figure 1 ;
- la figure 3 est un organigramme présentant un mode de mise en oeuvre du système de la figure 1.

Le mode de réalisation décrit ci-dessous est notamment destiné à être mis en oeuvre dans le cadre du projet européen Esprit numéro 7023 dénommé "CAFE". Il a notamment pour objectif de fournir un système de transaction sans contact à base de chèques électroniques cryptés.

La figure 1 illustre de façon simplifiée la structure du dispositif selon l'invention, ainsi que les éléments auxquels il peut être raccordés, ou avec lesquels il peut communiquer.

Le dispositif 11 comprend donc un microprocesseur 111, capable de le faire fonctionner, à partir des informations (programme, configuration ...) contenues dans une mémoire reprogrammable 112. Il comprend encore des moyens 113 permettant d'assurer la sécurisation de l'émission d'un chèque (codage de signatures cryptographiques basés sur des algorithmes à clés publiques, vérification de code confidentiel, module de sécurité sous la forme de "plug-in" ...) en tenant compte des informations (nombre de chèques et montant) contenues dans une mémoire de ressources de transaction 114, et des moyens 115 de communication sans contact, par exemple par infrarouge, avec un terminal de transactions 12. Ces moyens 115 peuvent par exemple mettre en oeuvre la norme IRDA ("InfraRed Data Association"), à 38400 bauds.

Par ailleurs, le dispositif 11 possède des moyens 116 de dialogue avec une ou plusieurs cartes à micro-circuits 13, par exemple selon la norme ISO 7816-3.

Selon un mode de réalisation particulier de l'invention, les moyens de dialogue 116 fonctionnent à une fréquence de transmission nominale prédéterminée (par exemple 7 MHz), qui peut être ramenée à une fréquence de transmission de repli correspondant à la moitié (soit la fréquence normalisée 3,5 MHz) si des problèmes dans les échanges de données sont détectés.

Les cartes 13 comprennent des moyens complets pour effectuer une transaction (indépendamment du dispositif 11) tels que des moyens de sécurisation 131 similaires aux moyens 113, une mémoire de ressources 132 et un microprocesseur 133.

Le dispositif 11 comporte un multiplexeur 117, ou tout autre moyen pour effectuer une sélection (celle-ci peut par exemple également être réalisée directement par le micro-processeur 111). Le multiplexeur 117 permet de choisir entre les moyens pour effectuer une transaction du dispositif ou ceux d'une carte. Dans les deux cas, la communication est assurée par les moyens de communication par infrarouge 115, sous le contrôle du micro-processeur 111. En revanche, la sécurisation de la transaction est intégralement prise en charge par l'élément (carte 13 ou dispositif 11) qui assure la transaction. Ainsi, lorsqu'il s'agit de la carte, le dispositif fonctionne de façon transparente, uniquement pour permettre une communication sans contact.

Le dispositif 11 comprend des moyens 118 pour détecter la présence d'une carte

dans les moyens de dialogue 116, et pour vérifier sa validité. Dans un mode de réalisation particulier de l'invention, ces moyens agissent directement sur le multiplexeur 117 pour sélectionner la carte dès qu'une carte valide est présente.

Une transaction peut notamment consister en l'émission d'un chèque ou en un rechargement des mémoires de ressource. Cette dernière opération s'effectue préférentiellement systématiquement dans la mémoire 114 du dispositif. Il est ensuite possible d'effectuer un transfert de cette mémoire 114 vers la mémoire 132 de la carte. D'autres types de transfert sont bien sûr possibles, en fonction des applications.

L'invention prévoit par ailleurs une technique avantageuse pour la maintenance ou la configuration (c'est-à-dire les opérations qui ne peuvent être effectuées que par des personnes habilitées) du dispositif 11. La personne habilitée dispose d'un détrompeur 14, qui présente le même format, ainsi que les mêmes contacts électriques, qu'une carte 12, de façon à pouvoir être inséré dans les moyens de dialogue 116. Ce détrompeur 14 comprend un moyen 141 qui permet au dispositif 11 de détecter qu'il s'agit d'une demande d'accès pour maintenance et non d'une carte classique. Ce moyen 141 est par exemple un détrompeur mécanique et/ou électrique.

Le détrompeur 14 comprend de plus avantageusement une alimentation 142 en une tension (par exemple 12 V) permettant d'effacer le contenu de la mémoire de programmation 112, afin de la reprogrammer. Cette tension d'effacement 142 est supérieure à la tension de fonctionnement du dispositif (par exemple 5 V).

Lorsque le détrompeur 14 est présent dans le dispositif 11, le microprocesseur 111 peut entrer en communication avec un terminal de maintenance 15. Préférentiellement, cette communication s'effectue selon le même protocole (infra-rouge) qu'une communication de transaction.

Selon un autre mode de réalisation, le détrompeur 14 peut comprendre directement l'intelligence (microprocesseur et mémoire), ou être une carte à micro-circuits spécifique, permettant la maintenance ou la configuration.

La figure 2 est un schéma synoptique plus détaillé d'un mode de réalisation du dispositif 11 .

Un microprocesseur 21 à faible consommation, par exemple du type MCU 8051

(marque déposée), gère le fonctionnement du dispositif, en fonction des informations stockées dans la mémoire 22 de programme et dans la mémoire 23 de données (qui sont accessibles lors des opérations de maintenance et de configuration indiquées ci-dessus).

Le microprocesseur 21 gère d'une part les relations avec les moyens de communication 25, comprenant l'interface infrarouge 251, et d'autre part l'interface homme/machine 26, qui comprend un clavier 261 (à 14 touches par exemple) et un écran 262 (par exemple de 2 lignes de 16 caractères, à cristaux liquides).

Cette interface homme/machine 26 permet de fournir de nombreux services nouveaux à l'utilisateur, tels que la consultation (visualisation du solde du dispositif et de la carte), la configuration et la personnalisation du dispositif,...

Une mémoire non-volatile 24 conserve les données correspondant aux ressources de transaction (nombre de chèques, montant disponible, montant maximum autorisé, chèques vierges,...).

La sécurisation 27 d'une transaction, lorsqu'elle est effectuée par le dispositif, est assurée préférentiellement par un coprocesseur cryptographique 271 relié au nùcroprocesseur 21 et par un module de sécurité 272. Ce module de sécurité a essentiellement pour but de protéger les intérêts de la banque. Il s'agit donc d'un module de surveillance (appelé encore "observer"), configuré dans un mode particulier et inaccessible pour les utilisateurs, qui conserve une image sécurisée du contenu de la mémoire de ressource (appelée également "purse"). Toute opération effectuée sur la mémoire de ressource affecte systématiquement ce module de surveillance. Il est à noter que la carte comprend également un tel système de sécurisation.

Lorsque la transaction est effectuée par une carte, le microprocesseur 21 est relié à l'interface 28 avec la carte. De façon à n'utiliser qu'un seul bus d'accès au microprocesseur 2 1, un multiplexeur 29 associe à ce bus soit l'interface 28, si une carte est présente, soit le module de sécurité 272.

La figure 3 présente un exemple de fonctionnement du système décrit ci-dessus. On distingue deux modes de fonctionnement (30) : le mode connecté, lorsque le dispositif coopère par infrarouge avec un terminal, et le mode non-connecté, lorsqu'il fonctionne de façon autonome. Les opérations possibles sont bien sûr différentes selon le

mode.

Toute opération en mode connecté commence, bien sûr, par l'établissement 31 d'une connexion entre un terminal et le dispositif portatif. La communication à établir est bi-directionnelle, mais la procédure 31 est préférentiellement non symétrique. Il s'agit d'une procédure maître-esclave, le terminal jouant le rôle du maître.

Cette procédure peut par exemple être la suivante :

- le maître (terminal) boucle sur l'émission d'un même paquet de données prédéfini dans la zone de communication avec les dispositifs ;
- l'esclave (dispositif) a deux possibilités :
  - s'il est en fonction en dehors d'une zone de communication : il est en mode non connecté ;
  - s'il est mis en fonction ou introduit en fonction dans une zone de communication, il reste en fonction et émet une réponse par son interface de communication, de façon à établir la connexion avec le maître (mode connecté).

Dans ce dernier cas, l'échange de messages peut débuter, et la communication bi-directionnelle reste activée jusqu'à ce que le dispositif-esclave soit éteint ou sorti de la zone de communication, ou jusqu'à ce que l'échange de données soit normalement arrêté par le terminal-maître.

Dans la pratique, lorsqu'on le met sous tension, le dispositif effectue systématiquement un test de connexion, pour déterminer s'il se trouve ou non dans une zone de communication. Il répète ensuite régulièrement ce test.

Une fois la connexion établie, au moins trois types d'opérations sont possibles (32) : le paiement, le rechargement et la maintenance. Les deux premières, appelées transactions, sont effectuées par le porteur du dispositif. La troisième est réservée à des personnes habilitées.

En ce qui concerne le paiement, il a été choisi d'utiliser prioritairement la carte, lorsque cela est possible. On vérifie donc la présence 33 d'une carte, puis la validité 34 de celle-ci. En cas de réponses favorables, un paiement par carte 35 est effectué. Dans le cas contraire, on réalise un paiement par le dispositif 36.

Plusieurs techniques sont possibles pour assurer le paiement 35, 36. Elles peuvent être identiques ou différentes selon que l'on utilise la carte ou le dispositif. Le déroulement peut par exemple être le suivant :

- le terminal communique au dispositif le montant à payer, éventuellement dans plusieurs devises ;
- le dispositif affiche ces données pour que l'utilisateur connaisse la somme à payer, dans plusieurs devises possibles, et les vérifie ;
- l'utilisateur accepte (dans une devise choisie) ou refuse la transaction grâce au clavier du dispositif. En cas de refus, la procédure est terminée (37) ;
- en cas d'acceptation, le terminal vérifie dans sa mémoire de ressources les autorisations accordées à l'utilisateur (montant maximum ou autorisation de paiement par exemple). Si l'un des éléments manque, la procédure est terminée (37) ;
- sinon, un chèque est émis par le dispositif, avec sécurisation des données qu'il contient, à l'aide d'une signature cryptographique ;
- le terminal vérifie la validité du chèque qu'il a reçu, par exemple en contrôlant à partir d'une clé publique sa signature cryptographique, puis accepte la transaction, si le chèque est validé. Sinon, la transaction est annulée.

Le rechargement 38 s'effectue entre le terminal et la mémoire de ressources du dispositif, selon une procédure similaire à celle décrite ci-dessus pour le paiement. Il est possible de recharger en chèques vierges et en montant(s) financier(s), éventuellement dans plusieurs devises.

La maintenance et la configuration 312 n'étant permises qu'aux personnes habilitées, le dispositif vérifie (311) la présence du détrompeur. Si le détrompeur est présent, un dialogue peut être établi avec un terminal de configuration, par l'intermédiaire des moyens de communication infrarouge. Avantageusement, le protocole de communication permet d'accéder directement à la plupart des composants formant le dispositif, pour des opérations de configuration ou de miantenance.

En mode non connecté, trois grands types d'opérations 39 sont également possibles : l'interrogation, le transfert de ressources et la configuration.

L'interrogation 310 permet par exemple de consulter le solde du compte (ou des comptes, lorsque plusieurs comptes dans plusieurs devises sont gérés) sur la carte et/ou sur le dispositif, ainsi que de visualiser la liste des dernières transactions effectuées et mémorisées, ou les taux de change.

La configuration 313 permet de personnaliser le dispositif et la carte, notamment en :

- changeant le code confidentiel du dispositif ou de la carte ;
- choisissant la langue d'utilisation du dispositif ;
- choisissant la monnaie utilisée pour les transactions.

Enfin, le transfert de ressources (chèques vierges et/ou montants) peut se faire (314) de la carte vers le dispositif 315 (par exemple lorsqu'on veut se débarrasser du reliquat d'une carte), ou du dispositif vers la carte 316 (par exemple lorsque l'on vient de recharger 38 le dispositif). Il est également envisageable d'effectuer des transferts de chèques crédités d'un montant choisi, d'une carte vers un dispositif et vice-versa (notamment de façon à effectuer une transaction entre deux personnes, l'une étant titulaire du dispositif et l'autre de la carte).

REVENDICATIONS

1. Dispositif portatif (11) destiné à effectuer des transactions sécurisées avec des terminaux de transaction (12), comprenant des premiers moyens (111, 113 ; 21, 271, 272) permettant la réalisation d'une transaction sécurisée, à partir de premières ressources de transaction stockées dans une première mémoire (114 ; 24), et des moyens (115 ; 25) de communication sans contact avec lesdits terminaux de transaction (12),

caractérisé en ce qu'il comprend des moyens (116 ; 28) de dialogue avec une carte à micro-circuits (13) comprenant des seconds moyens (131, 133) permettant la réalisation d'une transaction sécurisée, et des moyens (117 ; 29) de sélection entre lesdits premiers moyens de transaction sécurisée et lesdits seconds moyens de transaction sécurisée, tenant compte notamment d'informations représentatives de la présence et de la validité de ladite carte,

de façon qu'une transaction puisse être réalisée soit par ledit dispositif portatif (11), soit par ladite carte à micro-circuits (14), l'échange de données avec lesdits terminaux de transaction (12) étant dans les deux cas assuré par lesdits moyens (115 ; 25) de communication sans contact.

2. Dispositif selon la revendication 1, caractérisé en ce que lesdits premiers moyens de transaction sécurisée et/ou lesdits seconds moyens de transaction sécurisée assurent l'émission de chèques électroniques portant un montant transmis par un terminal de transaction, et authentifiés par une signature cryptée à l'aide d'un algorithme à clé publique, lesdits chèques étant stockés sous forme vierge dans une mémoire réinscriptible (24).

3. Dispositif selon l'une quelconque des revendications 1 et 2, caractérisé en ce qu'il comprend des moyens de rechargement en ressources de transaction dudit dispositif, par une communication sans contact avec un terminal de rechargement.

4. Dispositif selon l'une quelconque des revendications 1 à 3, caractérisé en ce qu'il comprend des moyens de transfert de ressources de transaction dudit dispositif vers une desdites cartes à micro-circuits et/ou d'une desdites cartes à micro-circuits vers ledit dispositif.

5. Dispositif selon l'une quelconque des revendications 1 à 4, caractérisé en ce que

lesdits moyens de dialogue peuvent recevoir un élément (14) de contrôle de configuration et/ou de maintenance comprenant des moyens (141) pour le distinguer d'une desdites cartes à microcircuits, et autorisant la configuration et/ou la maintenance dudit dispositif à partir d'un terminal de contrôle (15), par l'intermédiaire desdits moyens (115) de communication sans contact.

6. Dispositif selon l'une quelconque des revendications 1 à 4, caractérisé en ce que lesdits moyens de dialogue peuvent recevoir un élément (14) de configuration et/ou de maintenance comprenant des moyens (141) pour le distinguer d'une desdites cartes à microcircuits, et assurant la configuration et/ou la maintenance dudit dispositif.

7. Dispositif selon l'une quelconque des revendications 5 et 6, caractérisé en ce que ledit élément de contrôle ou ledit élément de configuration et/ou de maintenance délivre une tension électrique (142) supérieure à la tension électrique de fonctionnement dudit dispositif, et permettant d'effacer et de reprogrammer le contenu d'une mémoire reprogrammable.

8. Dispositif selon l'une quelconque des revendications 1 à 7, caractérisé en ce que lesdits moyens de communication sans contact sont des moyens (251) de communication bidirectionnels par infrarouge.

9. Dispositif selon l'une quelconque des revendications 1 à 8, caractérisé en ce que lesdits moyens de dialogue (116 ; 28) avec une carte à micro-circuits fonctionnent à une fréquence de transmission nominale prédéterminée, et en ce qu'ils comprennent des moyens de détection de défauts de transmission, entraînant le passage à une fréquence de transmission de repli correspondant à la moitié de ladite fréquence de transmission nominale.

10. Dispositif selon l'une quelconque des revendications 1 à 9, caractérisé en ce qu'il comprend un multiplexeur (29) associant à un port unique d'accès à un microprocesseur (21) de contrôle soit lesdits moyens (28) de dialogue avec une carte à micro-circuits, soit des moyens (272) de sécurisation interne d'une transaction.

11. Dispositif selon la revendication 10, caractérisé en ce que ledit multiplexeur (29) connecte systématiquement lesdits moyens (28) de dialogue avec une carte à micro-circuits lorsque la présence d'une carte valide est détectée.

12. Procédé de mise en oeuvre d'un dispositif portatif destiné à effectuer des transactions sécurisées avec des terminaux de transaction, caractérisé en ce qu'il prévoit deux modes de fonctionnement:

- un mode direct, dans lequel la transaction est gérée par ledit dispositif portatif ; et
- un mode transparent, dans lequel la transaction est gérée par une carte à micro-circuits couplée opérationnellement audit dispositif,

une communication sans contact avec lesdits terminaux de transaction étant mise en oeuvre de façon identique dans les deux modes.

13. Procédé selon la revendication 12, caractérisé en ce que ladite communication sans contact est une communication par infrarouge du type maître-esclave, le terminal de transaction jouant le rôle du maître et ledit dispositif jouant le rôle de l'esclave.

14. Procédé selon l'une quelconque des revendications 12 et 13, caractérisé en ce qu'il met en oeuvre au moins une des opérations consistant à :

- assurer l'émission de chèques électroniques portant un montant transmis par un terminal de transaction ;
- sécuriser un chèque par la transmission d'une signature cryptographique ;
- gérer au moins deux soldes correspondant à des devises différentes, de façon à permettre le paiement dans plusieurs devises et/ou à transcrire des montants transmis dans plusieurs devises ;
- assurer le dépôt et/ou le retrait d'un montant sur un compte ;
- valider l'utilisateur du dispositif et/ou de la carte à l'aide d'un code confidentiel ;
- recharger en chèques vierges et/ou en un montant financier ledit dispositif ;
- transférer des chèques (vierges ou crédités) et/ou un montant financier dudit dispositif vers une desdites cartes à micro-circuits et/ou d'une desdites cartes à micro-circuits vers ledit dispositif ;
- consulter un solde (montants et chèques) dudit dispositif et/ou d'une desdites cartes, une liste des dernières transactions et/ou des taux de change ;
- configurer et personnaliser le fonctionnement dudit dispositif.

1/2

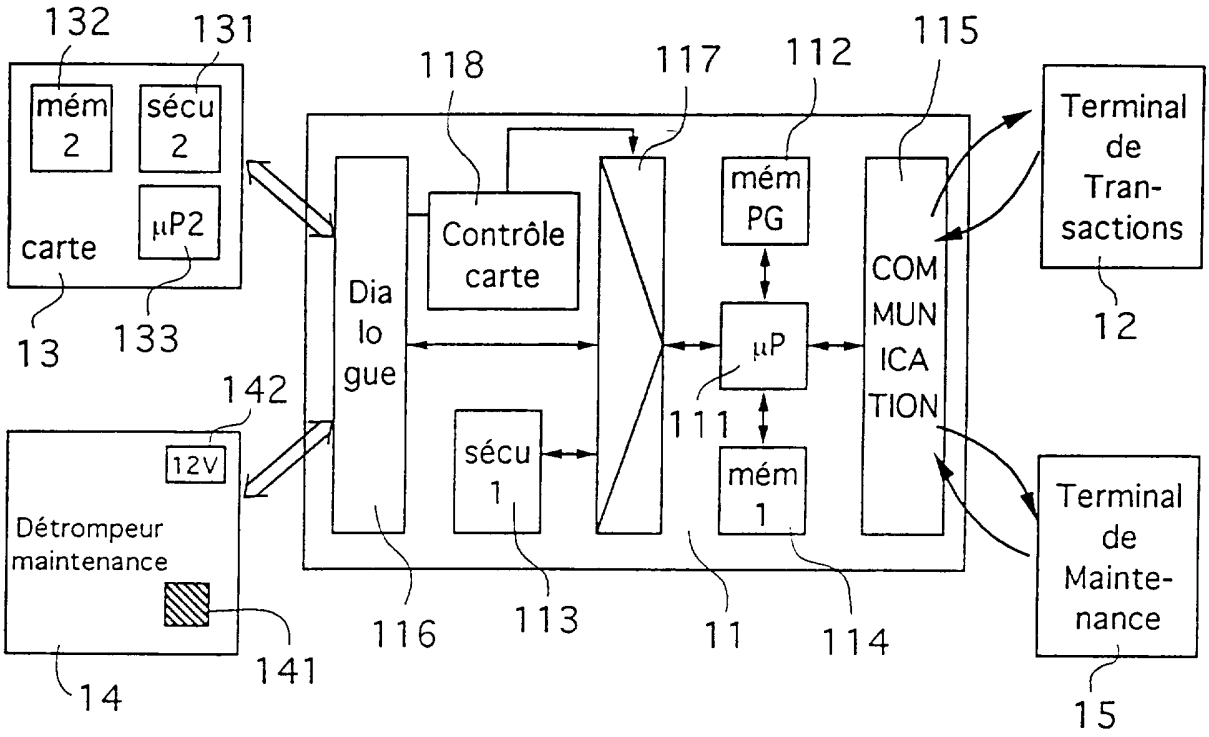

132
131
mém 2
sécu 2
µP2
carte
13
133
142
12V
Détrompeur maintenance
14
141
118
117
112
115
Contrôle carte
Dia lo gue
116
113
sécu 1
mém PG
µP
111
mém 1
11
114
COM MUN ICA TION
Terminal de Tran- sactions
12
Terminal de Mainte- nance
15

Fig. 1

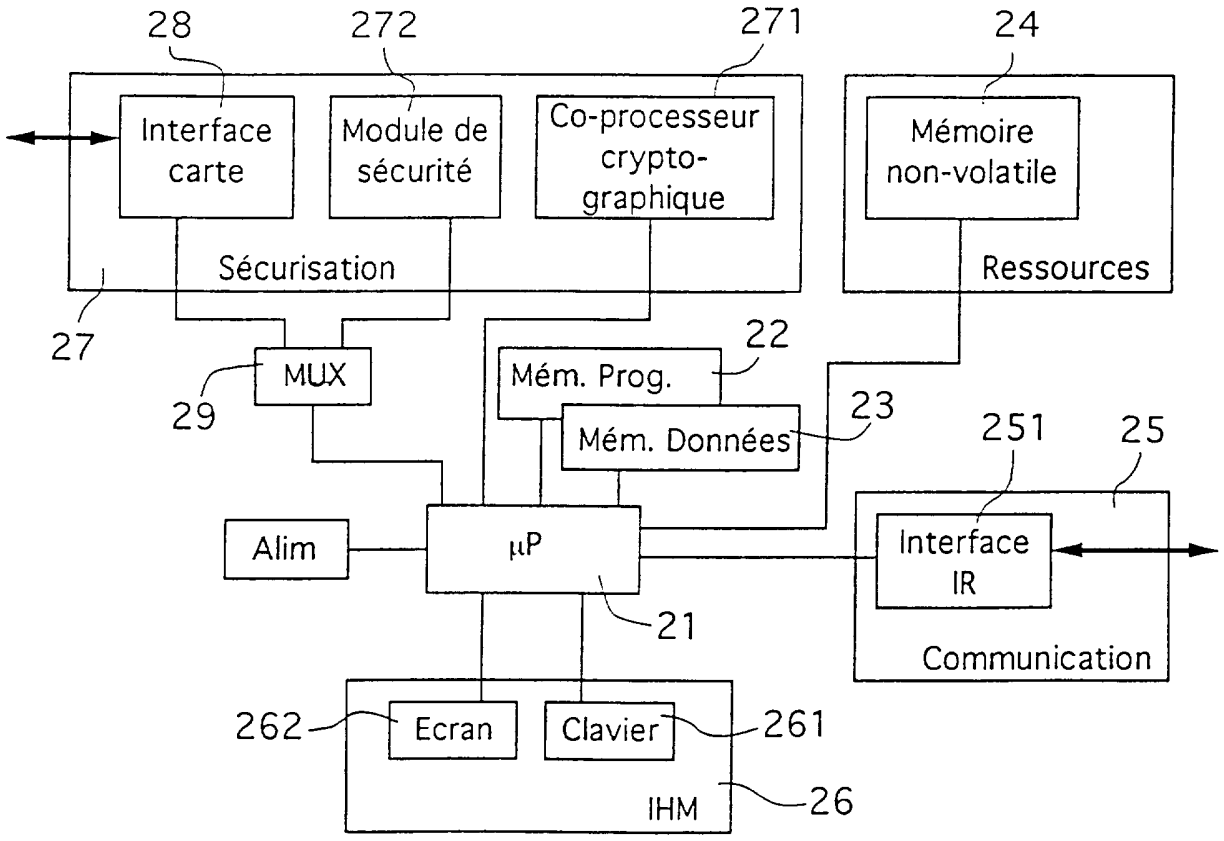

28
272
271
24
Interface carte
Module de sécurité
Co-processeur crypto- graphique
Sécurisation
Mémoire non-volatile
Ressources
27
MUX
29
22
Mém. Prog.
Mém. Données
23
251
25
Alim
µP
21
Interface IR
Communication
262
Ecran
Clavier
261
IHM
26

Fig. 2

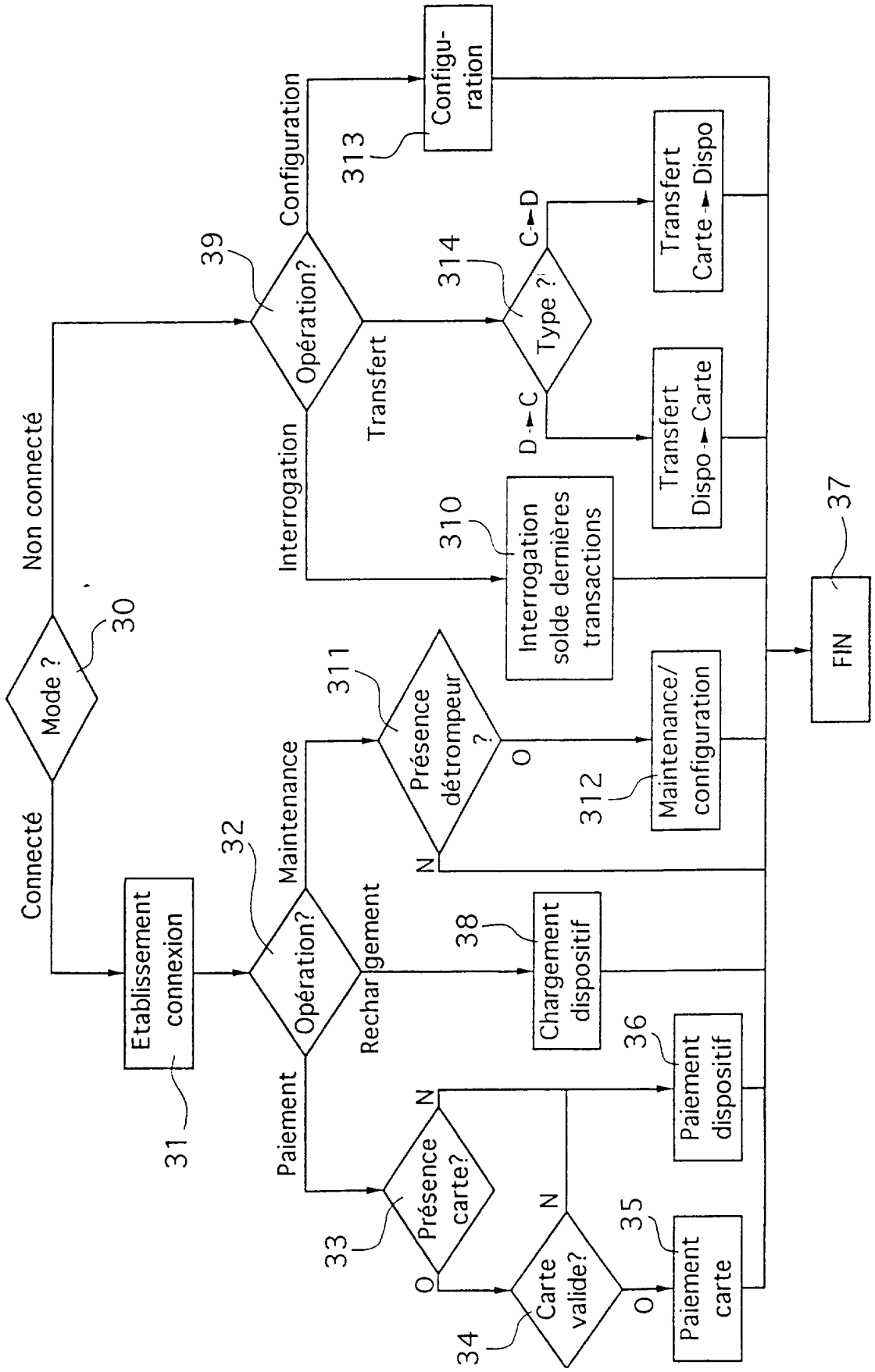

Mode ?
30
Non connecté
Connecté
Etablissement connexion
31
Opération?
32
Maintenance
Rechargement
Paiement
Présence détrompeur ?
311
O
N
Maintenance/ configuration
312
Chargement dispositif
38
Présence carte?
33
O
N
Carte valide?
34
N
O
Paiement dispositif
36
Paiement carte
35
Opération?
39
Configuration
Transfert
Interrogation
Configu- ration
313
Type ?
314
C→D
D→C
Transfert Carte→Dispo
Transfert Dispo→Carte
Interrogation solde dernières transactions
310
FIN
37

Fig. 3

INTERNATIONAL SEARCH REPORT

International Application No
PC1/FR 96/01583

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/10 G06K19/073

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

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	WO,A,85 04035 (CORPRA RESEARCH,INC.) 12 September 1985 see claims 6-8,12,21,24 ---	1-4,8, 12-14
Y	US,A,4 277 837 (STUCKERT,P.E.) 7 July 1981 see claims 1,2,4 ---	1-4,8, 12-14
A	EP,A,0 565 469 (INNOVATRON INDUSTRIES) 13 October 1993 see claims 1,12 ---	1-4, 12-14
A	FR,A,2 636 153 (PARIENTI,R.) 9 March 1990 see the whole document ---	1-4,8,13
A	FR,A,2 637 710 (B + DEVELOPMENT) 13 April 1990 see claims 1,5,12 -----	1,4,14

☐ 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
6 February 1997	14.02.97

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	Herskovic, M

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

INTERNATIONAL SEARCH REPORT

.ıformation on patent family members

Inter ›nal Application No
PC ı/FR 96/01583

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
WO-A-8504035	12-09-85	US-A-	4575621	11-03-86
		AU-A-	4117885	24-09-85
		EP-A-	0173741	12-03-86
US-A-4277837	07-07-81	CA-A-	1111567	27-10-81
		DE-A-	2852941	05-07-79
		FR-A-	2413721	27-07-79
		GB-A,B	2011671	11-07-79
		JP-C-	1220759	26-07-84
		JP-A-	54094855	26-07-79
		JP-B-	58053784	01-12-83
		NL-A-	7812390	03-07-79
		SE-A-	7812924	01-07-79
EP-A-565469	13-10-93	FR-A-	2689997	15-10-93
		BR-A-	9301486	13-10-93
		CA-A-	2093267	09-10-93
		JP-A-	6089244	29-03-94
FR-A-2636153	09-03-90	FR-A-	2632752	15-12-89
		AU-A-	3832689	05-01-90
		EP-A-	0402182	12-12-90
		WO-A-	8912288	14-12-89
		JP-T-	3501180	14-03-91
FR-A-2637710	13-04-90	NONE		

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 96/01583

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 G07F7/10 G06K19/073

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

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relevent 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	WO,A,85 04035 (CORPRA RESEARCH,INC.) 12 Septembre 1985 voir revendications 6-8,12,21,24	1-4,8, 12-14
Y	US,A,4 277 837 (STUCKERT,P.E.) 7 Juillet 1981 voir revendications 1,2,4	1-4,8, 12-14
A	EP,A,0 565 469 (INNOVATRON INDUSTRIES) 13 Octobre 1993 voir revendications 1,12	1-4, 12-14
A	FR,A,2 636 153 (PARIENTI,R.) 9 Mars 1990 voir le document en entier	1-4,8,13
A	FR,A,2 637 710 (B + DEVELOPMENT) 13 Avril 1990 voir revendications 1,5,12	1,4,14

☐ 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'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

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
6 Février 1997	14.02.97

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	Herskovic, M

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs au[illegible]embres de familles de brevets

Demande Internationale No
PCT/FR 96/01583

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO-A-8504035	12-09-85	US-A-	4575621	11-03-86
		AU-A-	4117885	24-09-85
		EP-A-	0173741	12-03-86
US-A-4277837	07-07-81	CA-A-	1111567	27-10-81
		DE-A-	2852941	05-07-79
		FR-A-	2413721	27-07-79
		GB-A,B	2011671	11-07-79
		JP-C-	1220759	26-07-84
		JP-A-	54094855	26-07-79
		JP-B-	58053784	01-12-83
		NL-A-	7812390	03-07-79
		SE-A-	7812924	01-07-79
EP-A-565469	13-10-93	FR-A-	2689997	15-10-93
		BR-A-	9301486	13-10-93
		CA-A-	2093267	09-10-93
		JP-A-	6089244	29-03-94
FR-A-2636153	09-03-90	FR-A-	2632752	15-12-89
		AU-A-	3832689	05-01-90
		EP-A-	0402182	12-12-90
		WO-A-	8912288	14-12-89
		JP-T-	3501180	14-03-91
FR-A-2637710	13-04-90	AUCUN		