Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2219823 C 2007/07/17

(11)(21) 2 219 823

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(86) Date de dépôt PCT/PCT Filing Date: 1996/05/28
(87) Date publication PCT/PCT Publication Date: 1996/12/05
(45) Date de délivrance/Issue Date: 2007/07/17
(85) Entrée phase nationale/National Entry: 1997/11/20
(86) N° demande PCT/PCT Application No.: FR 1996/000797
(87) N° publication PCT/PCT Publication No.: 1996/038826
(30) Priorité/Priority: 1995/05/30 (FR95/06371)

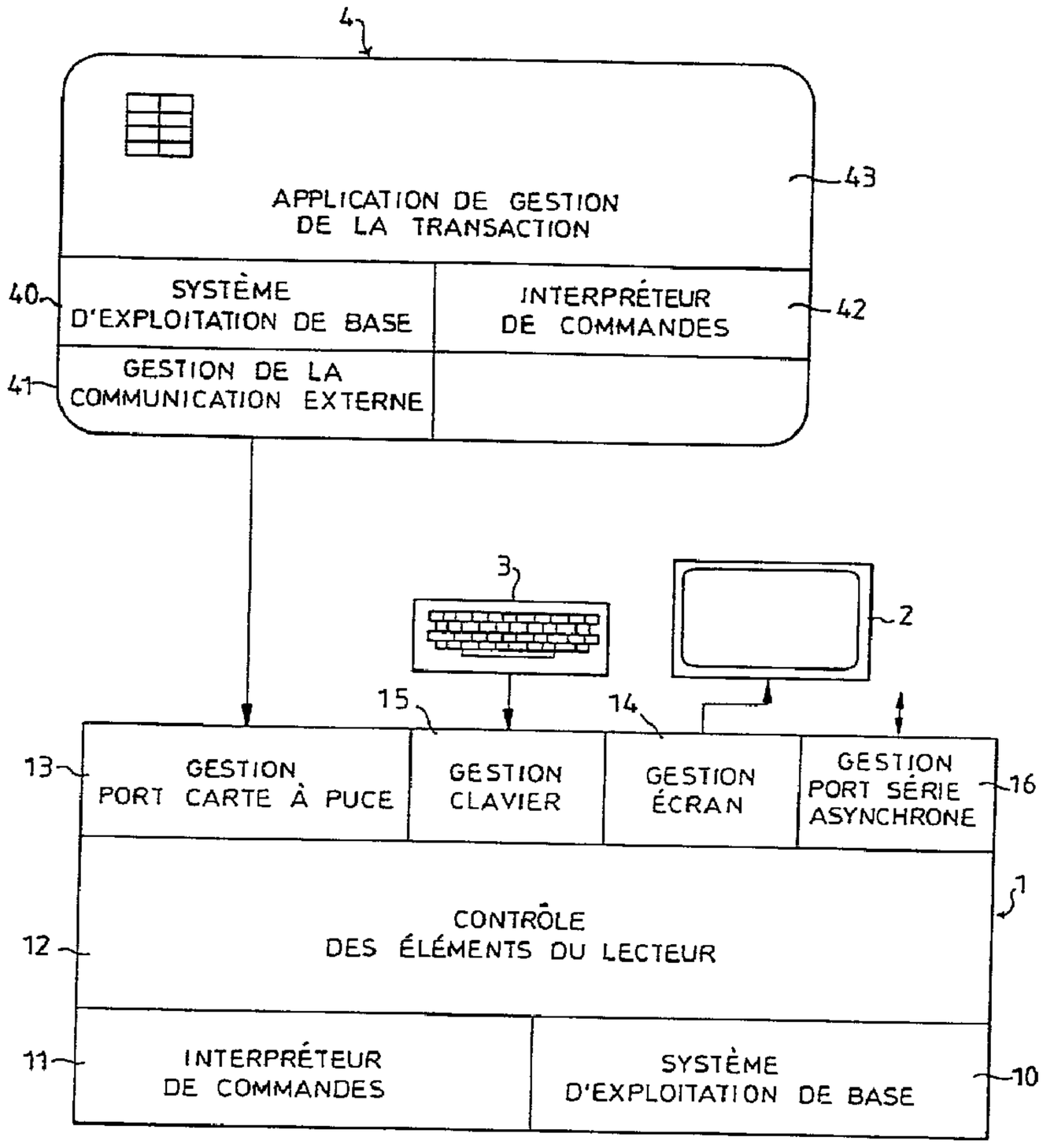
(51) Cl.Int./Int.Cl. *G07F 7/08* (2006.01), *G06K 19/07* (2006.01), *G06K 7/00* (2006.01), *G07F 7/10* (2006.01)

(72) Inventeurs/Inventors:
CESAIRE, GERARD, FR;
DEVAUX, FRANCOIS, FR;
GERARD, YVES, FR

(73) Propriétaire/Owner:
OBERTHUR CARD SYSTEMS SA, FR

(74) Agent: ROBIC

(54) Titre : SYSTEME A CARTES A PUCE INTELLIGENTES
(54) Title: SMART CARD SYSTEM



(57) Abrégé/Abstract:
Les cartes à puce intelligentes sont celles qui contrôlent elles-mêmes de déroulement de leur transaction, afin d'éviter de spécialiser un lecteur de carte à puce par type de transaction. Le système à cartes à puce intelligentes concerné comporte au

CA 2219823 C 2007/07/17

(11)(21) 2 219 823

(13) C

(57) Abrégé(suite)/Abstract(continued):
moins un lecteur (1) de carte à puce et une carte à puce (4) stockant en mémoire un programme de gestion de transaction. Il est remarquable en ce que le lecteur (1) contrôle des cycles d'échange en envoyant à la carte à puce (4) de manière alternative et répétitive, d'une part une requête de mise à disposition d'un paquet d'instructions et de données dit "message carte" et, d'autre part, une déclaration de compte rendu associée à un message de compte rendu sur l'exécution, par le lecteur (1), d'instructions précédemment reçues dans des messages carte, et en ce que la carte à puce (4) contrôle des cycles de traitement synchrones des cycles d'échange grâce à des moyens d'exécution d'un programme de gestion de transaction élaborant les instructions et données des messages carte au rythme des requêtes de mise à disposition de message carte et des déclarations de compte rendu émises par le lecteur (1).

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 7/00

A1

(11) Numéro de publication internationale: **WO 96/38826**

(43) Date de publication internationale: 5 décembre 1996 (05.12.96)

(21) Numéro de la demande internationale: PCT/FR96/00797

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

(30) Données relatives à la priorité:
95/06371 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]; Thomson-CSF S.C.P.I., Boîte postale 329, F-92402 Courbevoie Cédex (FR). DEVAUX, François [FR/FR]; Thomson-CSF S.C.P.I., Boîte postale 329, F-92402 Courbevoie Cédex (FR). GERARD, Yves [FR/FR]; Thomson-CSF S.C.P.I., Boîte postale 329, F-92402 Courbevoie Cédex (FR).

(74) Mandataire: THOMSON-CSF S.C.P.I.; 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: SMART CARD SYSTEM

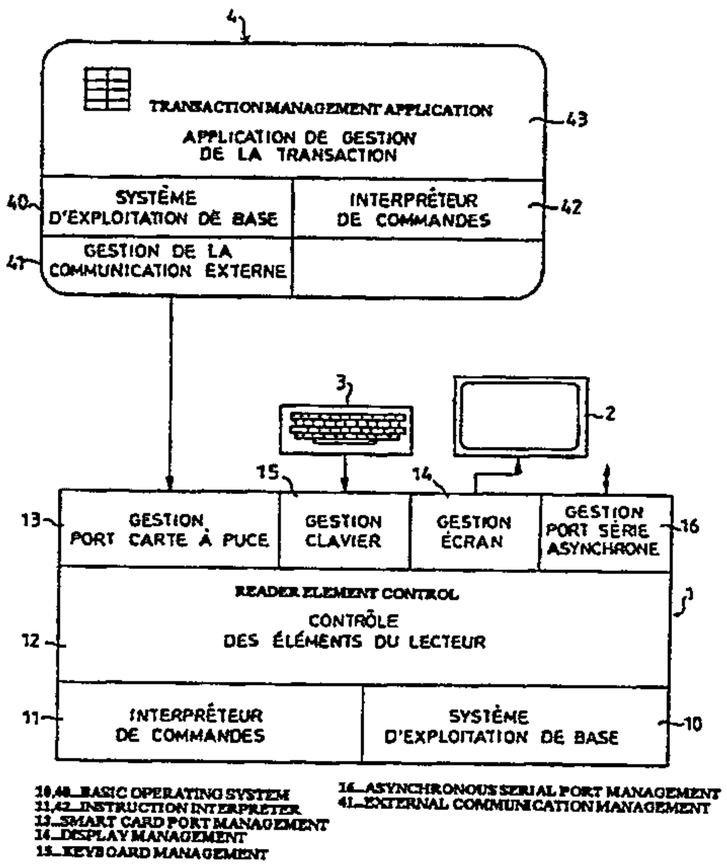
(54) Titre: SYSTEME A CARTES A PUCE INTELLIGENTES

(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 smart card system of the invention has at least one card reader (1) and a smart card (4) storing a transaction management programme. The system is characterised in that the reader (1) controls the exchange cycles by alternately and repetitively sending to the card (4) a request for issuing an instruction and data packet designated as "card message", and a report statement associated with a report message relating to the execution of previously received instructions in card messages by the reader. The smart card (4) controls the processing cycles which are synchronous with the exchange cycles through transaction management programme execution means which develop the instructions and data of the card messages at the rate of the card message issue requests and of report statements transmitted by the reader (1).

(57) Abrégé

Les cartes à puce intelligentes sont celles qui contrôlent elles-mêmes de déroulement de leur transaction, afin d'éviter de spécialiser un lecteur de carte à puce par type de transaction. Le système à cartes à puce intelligentes concerné comporte au moins un lecteur (1) de carte à puce et une carte à puce (4) stockant en mémoire un programme de gestion de transaction. Il est remarquable en ce que le lecteur (1) contrôle des cycles d'échange en envoyant à la carte à puce (4) de manière alternative et répétitive, d'une part une requête de mise à disposition d'un paquet d'instructions et de données dit "message carte" et, d'autre part, une déclaration de compte rendu associée à un message de compte rendu sur l'exécution, par le lecteur (1), d'instructions précédemment reçues dans des messages carte, et en ce que la carte à puce (4) contrôle des cycles de traitement synchrones des cycles d'échange grâce à des moyens d'exécution d'un programme de gestion de transaction élaborant les instructions et données des messages carte au rythme des requêtes de mise à disposition de message carte et des déclarations de compte rendu émises par le lecteur (1).



SYSTEME A CARTES A PUCE INTELLIGENTES

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, agencés pour permettre le déroulement d'une transaction par exemple bancaire ou santé.

La présente invention est relative à un système formé par une carte à puce et un lecteur de carte à puce qui permet d'exécuter la transaction à laquelle est dédiée la carte à puce.

Les systèmes connus à cartes à puce et lecteur comportent d'une part des cartes à puce dotées de mémoires et éventuellement d'un microcontrôleur, et utilisées uniquement comme support de données agrémenté de moyens de sécurisation et, d'autre part, des lecteurs de carte à puce pourvus d'une intelligence suffisante pour contrôler le déroulement de la transaction envisagée.

Les lecteurs de carte à puce sont équipés d'un système assurant une liaison avec une carte à puce soit au moyen d'un connecteur électrique à broche multiple, soit au moyen d'une antenne capacitive ou inductive. Ils peuvent être autonomes et se suffire à eux mêmes ou transparents et servir d'accès à un système informatique. Lorsqu'ils sont autonomes, ils comportent des éléments de communication suffisants pour permettre à une personne de suivre les étapes d'une transaction : clavier et afficheur qui sont gérés, de même que la liaison avec la carte à puce, par un microcontrôleur propre au lecteur doté d'un programme d'application spécifique de la transaction envisagée. Lorsqu'ils sont transparents, ils se comportent comme un simple port d'entrée-sortie, spécialisé pour une carte à puce, vis à vis d'un système informatique programmé spécialement pour la transaction envisagée. Dans les deux cas, ils transmettent à la carte à puce des instructions mises sous une forme respectant un protocole d'échange spécifique qui est souvent celui défini dans la norme ISO7816-3, et la carte à puce se contente d'exécuter ces instructions et de rendre compte.

L'intelligence de la transaction est située soit au niveau du lecteur, soit à celui du système informatique associé au lecteur. Cela 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 également changer la programmation du lecteur, s'il est autonome, ou celle 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 qui alors stocke en mémoire le programme de gestion de la transaction et le fait exécuter.

Le lecteur devient alors un organe extérieur dont la fonction principale est de fournir les ressources nécessaires à la réalisation de la transaction et notamment de mettre à disposition de la carte à puce des interfaces tels que clavier, afficheur, liaison asynchrone et moyen de liaison à une autre carte à puce ou à un système informatique.

Il se pose alors le problème de faire parvenir au lecteur certaines instructions à effectuer en relation avec le programme de gestion de la transaction stocké en mémoire dans la carte à puce et déroulé par celle-ci.

Pour résoudre ce problème, il est connu, par exemple par la demande européenne de brevet EP-A-0 490 455, de définir un protocole de communication entre carte à puce et lecteur de carte à puce utilisant un petit nombre de commandes spécifiques de certaines actions demandées au lecteur par une carte à puce, et de requêtes et réponses de la part du lecteur compatibles avec ces commandes, ayant des caractéristiques assez générales pour convenir à différentes sortes de cartes à puce et de lecteurs. Cette solution présente cependant l'inconvénient de limiter à un cadre assez étroit dû à la spécificité des commandes, requêtes et réponses, les possibilités et la nature des échanges entre une carte à puce et son lecteur. Elle a aussi l'inconvénient de ne plus respecter les normes existantes sur la gestion des communications entre une carte à puce et un lecteur de carte à puce et par conséquent d'être incompatible avec la génération précédente de cartes à puce.

La présente invention a pour but un protocole de communication entre une carte à puce intelligente et un lecteur de carte à puce qui impose le moins possible de limitation aux échanges entre une carte à puce et son lecteur afin d'éviter une spécialisation du lecteur de carte à puce à un type particulier de carte à puce, et qui soit facile à mettre en accord avec les

normes existant sur la gestion des communications entre une carte à puce et son lecteur.

Elle a pour objet un système pour cartes à puce intelligentes comportant au moins un lecteur de carte à puce pourvu de moyens d'alimentation de carte à puce activés par la connexion d'une carte à puce et une carte à puce stockant en mémoire un programme de gestion de transaction. Ce système est remarquable en ce que le lecteur de carte à puce comporte :

- des moyens engendrant de manière alternative et répétitive, à destination d'une carte à puce raccordée, d'une part une requête de mise à disposition d'un paquet d'instructions et de données élaborées au sein de ladite 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, par le lecteur, d'instructions reçues précédemment dans des messages carte de

ladite carte à puce, la déclaration de compte rendu et le message de compte rendu étant dits "compte rendu lecteur",

- des moyens de réception et de traitement du message carte délivré par ladite carte à puce à la suite d'une requête de mise à disposition d'un message carte, et

- des moyens d'élaboration et de transmission de messages de compte rendu lecteur à la suite d'une exécution d'instructions reçues de ladite carte à puce dans des messages carte,

et en ce que ladite carte à puce comporte :

- des moyens d'initialisation activés à la mise sous tension de ladite carte à puce provoquant la mise à disposition dudit lecteur d'un premier message carte,

- des moyens de reconnaissance d'une requête de mise à disposition d'un message carte émanant dudit lecteur et de transmission de message carte à destination dudit lecteur en réponse à une telle requête de mise à disposition d'un message carte,

- des moyens de reconnaissance d'une déclaration de compte rendu et de traitement du message de compte rendu associé en provenance dudit lecteur, et

- des moyens d'exécution dudit programme de gestion de transaction élaborant les instructions et données des messages carte au rythme des requêtes de mise à disposition de message carte et des déclarations de compte rendu émises par ledit lecteur.

Avantageusement, une requête de mise à disposition d'un message carte émanant du lecteur de carte à puce consiste en une commande du type "get response" normalement utilisée dans les normes ISO7816/prEN726 pour adresser, au lecteur, des données préparées, tandis qu'une déclaration de compte rendu émanant du lecteur consiste en une commande du type "enveloppe" ou "execute" normalement utilisée dans les normes ISO7816/prEN726 pour envoyer des données ou faire exécuter un programme au sein d'une carte à puce.

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 en regard du dessin dans lequel la figure unique illustre, de manière schématique, les différentes couches

logiques des programmes d'une carte à puce intelligente et du lecteur associé d'un système selon l'invention.

On distingue sur cette figure les grandes partitions des programmes de gestion des microcontrôleurs d'un lecteur 1 de carte à puce équipé avec un écran d'affichage 2 et un clavier 3, et d'une carte à puce intelligente 4.

Pour le lecteur 1, la couche la plus enfouie de son programme d'exploitation est un système d'exploitation de base 10, en code exécutable, adapté au type du microcontrôleur, qui gère sa mémoire. Ce système d'exploitation de base 10 est associé à un interpréteur de commandes 11 reconnaissant les différentes instructions en langage évolué susceptibles de se trouver dans un message carte. L'ensemble est surmonté d'une couche intercalaire constituée d'un programme de contrôle 12 assurant la maîtrise des divers éléments du lecteur et d'une couche externe constituée de divers programmes de gestion de périphériques dont un programme 13 de gestion de communication avec une carte à puce selon la norme ISO7816-3, un programme 14 de gestion d'écran d'affichage, un programme 15 de gestion de clavier et un programme 16 de gestion de port série asynchrone pour une éventuelle liaison avec un système informatique déporté. Le programme de contrôle 12 assure l'aiguillage des ordres provenant des messages carte vers l'interpréteur de commandes 11, la constitution des messages de compte rendu à destination de la carte à puce, l'élaboration de la succession des requêtes de mise à disposition de messages carte et des déclarations de compte rendu à destination de la carte à puce, et l'interface entre le système d'exploitation de base et les différents programmes de gestion des périphériques.

Pour la carte à puce intelligente 4, la couche la plus enfouie de son programme d'exploitation est encore un système d'exploitation de base 40, en code exécutable, adapté au type de microcontrôleur, qui gère sa mémoire, avec les systèmes habituels de sécurisation d'une carte à puce, et un protocole de communication externe 41. Ce système d'exploitation de base 40 est associé à un interpréteur de commandes 42 résidant en mémoire ROM et reconnaissant des ordres en langage évolué . L'ensemble du système d'exploitation de base 40 et de l'interpréteur de commandes 41 est surmonté par une couche externe constituée d'un programme en

langage évolué 43 de gestion de la transaction à laquelle est dédiée la carte à puce, qui est stocké en mémoire EEPROM.

Le lecteur 1 communique avec la carte à puce intelligente 4 au moyen d'une liaison à alternat grâce à une succession de cycles de deux commandes successives des normes ISO7816/prEN726 qui sont la commande "get response" et la commande "enveloppe" ou "execute".

La commande "get-response" est constituée par l'envoi du 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" donnant un compte rendu carte.

La commande "execute" est constituée par l'envoi du 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 4 dans le lecteur 1, la carte à puce se trouve détectée et mise sous tension par le lecteur 1 qui lui envoie un ordre de remise à zéro selon la norme ISO7816-3. Il en résulte un processus d'initialisation du microcontrôleur de la carte à puce 4 qui se termine par l'envoie au lecteur 1, depuis la carte à puce 4, 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 4 pour un premier cycle de traitement aboutissant dans cette dernière à la préparation du premier message carte qui pourra être communiqué au lecteur 1 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 1 entame un premier cycle d'échange de données avec la carte à puce 4.

Au cours de ce premier cycle d'échange, le lecteur 1 envoie en direction de la carte à puce 4 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 4 après son initialisation.

La carte à puce 4, à la réception d'une telle requête par la commande "get response" envoie le message carte préparé au lecteur 1.

Le lecteur 1 reçoit le message carte, identifie les données qu'il contient, interprète le message, exécute les commandes demandées et répond à la carte à puce 4 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 4 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 1, la carte à puce 4 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 1 entame ensuite un deuxième cycle d'échange en envoyant à la carte à puce 4 une deuxième commande "get response" pour lire le nouveau message carte. Après traitement des données de ce nouveau message carte, le lecteur 1 rend compte de son exécution à la carte à puce 4, 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 4, à la réception de cette deuxième commande "enveloppe" ou "execute" en provenance du lecteur 1, 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 1, puis prépare un autre message carte.

Le lecteur 1 entame alors un troisième cycle d'échange en envoyant à la carte à puce 4 une troisième commande "get response" pour recevoir ce message carte.

Les cycles de traitement, à l'initiative de la carte à puce 4, et d'échange, à l'initiative du lecteur 1, se succèdent ainsi en fonction du programme de gestion de la transaction stocké dans la carte à puce 4.

Conformément à la norme ISO7816-3 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.

Dans le cas où le système comporte plusieurs cartes à puce, une seule carte à la fois pilote la transaction. La carte à puce qui pilote la transaction est dite "active". Les autres sont dites "passives". La carte à puce déclarée active est la première qui est capable de fournir une réponse à une instruction "get response" du lecteur.

Comme cela a été mentionné précédemment, la commande "get response" est utilisée par le lecteur pour demander à la carte à puce qui a été déclarée "active", les types d'opération qu'il doit effectuer au cours d'une transaction.

Les types d'opérations qu'une carte à puce active peut demander au lecteur peuvent être assez divers. Parmi eux, on peut citer :

- une demande de la configuration du lecteur auquel le lecteur retourne un compte rendu résumant ses principales caractéristiques,
- un arrêt/relance du lecteur auquel le lecteur retourne un compte rendu donnant son état de fonctionnement,
- une installation d'un programme dans le lecteur grâce à des paramètres d'appel, contenus dans des messages carte, tels que : nom du programme, longueur et contenu du programme. A cette installation, le lecteur retourne un compte rendu sur son état et les données de l'installation effectuée.
- une exécution d'un programme installé grâce à des paramètres d'appel, contenus dans des messages carte, tels que : nom du programme, longueur des données, données d'appel du programme. A cette exécution, le lecteur retourne un compte rendu sur son état et la longueur des données en retour.
- une demande d'ouverture/fermeture de liaison asynchrone grâce à des paramètres d'appel, contenus dans des messages carte, tels que : numéro du port, identifiant du correspondant, sens. A cette demande le lecteur retourne un compte rendu sur l'état et le numéro du port concerné.

- une demande de visualisation d'un message opérateur grâce à des paramètres d'appel, contenus dans des messages carte, tels que : type de message (permanent, à acquitter,...), type de visualisation (fixe, clignotant,...), nombre d'éléments du message, coordonnées de chaque élément du message, longueur du libellé, libellé. A cette demande, le lecteur retourne un compte rendu d'état.

- une demande de sélection dans un menu grâce à des paramètres d'appel, contenus dans des messages carte, tels que : type de menu, nombre de lignes du menu, nom de la ligne, coordonnées de chacun des choix, libellé. A cette demande, le lecteur retourne un compte rendu indiquant le numéro de la ligne sélectionnée.

- une demande de saisie dans une grille grâce à des paramètres d'appel, contenus dans des messages carte, tels que : nom de la grille, type de la grille (initiale, enchaînement,...), nombre de questions, coordonnées du libellé de chaque question, coordonnée de chaque réponse, nombre maximum de caractères à saisir, type de champ (saisie obligatoire, non visualisé, non modifiable,...), longueur du libellé de la question, libellé de la question, nombre de caractères de la valeur par défaut de la réponse, valeur par défaut de la réponse (absente si la longueur vaut zéro). A cette demande, le lecteur retourne un compte rendu comportant soit :

- le nom de la grille, le numéro d'une question et une demande d'action complémentaire ou une valeur saisie,
- un abandon,
- le nom de la grille, une validation, la date et l'heure,

- une écriture dans un fichier du lecteur grâce à des paramètres d'appel, contenus dans des messages carte, tels que : nom du fichier, adresse dans le fichier, longueur des données à écrire et les données à écrire elles-mêmes. A cette demande, le lecteur retourne un compte rendu donnant l'état et le nom du fichier.

- une demande d'authentification externe avec en retour un compte rendu donnant la preuve de la validité du lecteur,

- un échange de données chiffrées/déchiffrées grâce à des paramètres d'appel, contenus dans des messages carte, tels que : longueur des données chiffrées/déchiffrées et données chiffrées/déchiffrées, avec un

compte rendu en retour du lecteur donnant le numéro de clef, la longueur des données et les données elles-mêmes,

- une demande de signature d'un fichier grâce à des paramètres d'appel, contenus dans des messages carte, tels que : le nom du fichier, avec en retour un compte rendu du lecteur donnant la signature demandée,

- une demande d'exécution d'une commande pour carte à puce passive grâce à des paramètres d'appel, contenus dans des messages carte, constitués de commandes au format carte passive selon la norme ISO7816-4, avec un compte rendu en retour donnant un état, la longueur des données en retour et les données en retour,

- une demande d'exécution d'une commande "standard" du lecteur grâce à des paramètres d'appel contenus dans des messages carte , avec un compte rendu lecteur.

On entend par commande "standard" lecteur, toute commande exécutable par le système d'exploitation du lecteur. Les commandes "standard" comprennent en particulier :

- une demande de création/destruction de répertoire dans la mémoire du lecteur,

- une demande de sélection d'un répertoire dans la mémoire du lecteur,

- une demande de lecture du contenu d'un répertoire du lecteur,

- une demande de création/destruction de fichiers dans le répertoire courant du lecteur,

- une demande de copie/sauvegarde/restauration de fichiers du lecteur vers un port de communication (carte à puce ou asynchrone),

- une demande de lancement d'un fichier exécutable,

- une installation d'un programme dans l'application lecteur à partir d'un fichier du lecteur,

- une demande d'impression si le lecteur est muni ou connecté à une imprimante,

- une demande de la date et de l'heure,

- .....

En outre le lecteur peut signaler lui-même certains événement externes :

- demande de connexion d'une liaison asynchrone (n° du port, identifiant du demandeur),
- insertion d'une carte (n° de la carte insérée, ATR),
- retrait d'une carte (n° de la carte extraite),
- inactivité du clavier,
- .....

REVENDICATIONS

1. Système pour cartes à puce intelligentes comportant au moins un lecteur (1) de carte à puce pourvu de moyens d'alimentation de carte à puce activés par la connexion d'une carte à puce et une carte à puce (4) stockant en mémoire un programme de gestion de transaction (43), ce système étant caractérisé en ce que le lecteur (1) de carte à puce comporte :

- des moyens engendrant de manière alternative et répétitive, à destination d'une carte à puce (4) raccordée, d'une part une requête de mise à disposition d'un paquet d'instructions et de données élaborées au sein de ladite carte à puce (4) dit "message carte" et, d'autre part, une déclaration de compte rendu associée à un message de compte rendu sur l'exécution, par le lecteur (1), d'instructions reçues précédemment dans des messages carte de ladite carte à puce (4), la déclaration de compte rendu et le message de compte rendu étant dits "compte rendu lecteur",

- des moyens de réception et de traitement du message carte délivré par ladite carte à puce (4) à la suite d'une requête de mise à disposition d'un message carte, et

- des moyens d'élaboration et de transmission de messages de compte rendu lecteur à la suite d'une exécution d'instructions reçues de ladite carte à puce (4) dans des messages carte,

et en ce que ladite carte à puce (4) comporte :

- des moyens d'initialisation activés à la mise sous tension de ladite carte à puce (4) provoquant la mise à disposition dudit lecteur (1) d'un premier message carte,

- des moyens de reconnaissance d'une requête de mise à disposition d'un message carte émanant dudit lecteur (1) et de transmission de message carte à destination dudit lecteur (1) en réponse à une telle requête de mise à disposition d'un message carte,

- des moyens de reconnaissance d'une déclaration de compte rendu et de traitement du message de compte rendu associé en provenance dudit lecteur (1), et

- des moyens d'exécution dudit programme de gestion de transaction élaborant les instructions et données des messages carte au

rythme des requêtes de mise à disposition de message carte et des déclarations de compte rendu émises par ledit lecteur (1).

2. Système selon la revendication 1, caractérisé en ce que les moyens d'exécution dudit programme de gestion de transaction élaborent des instructions de :

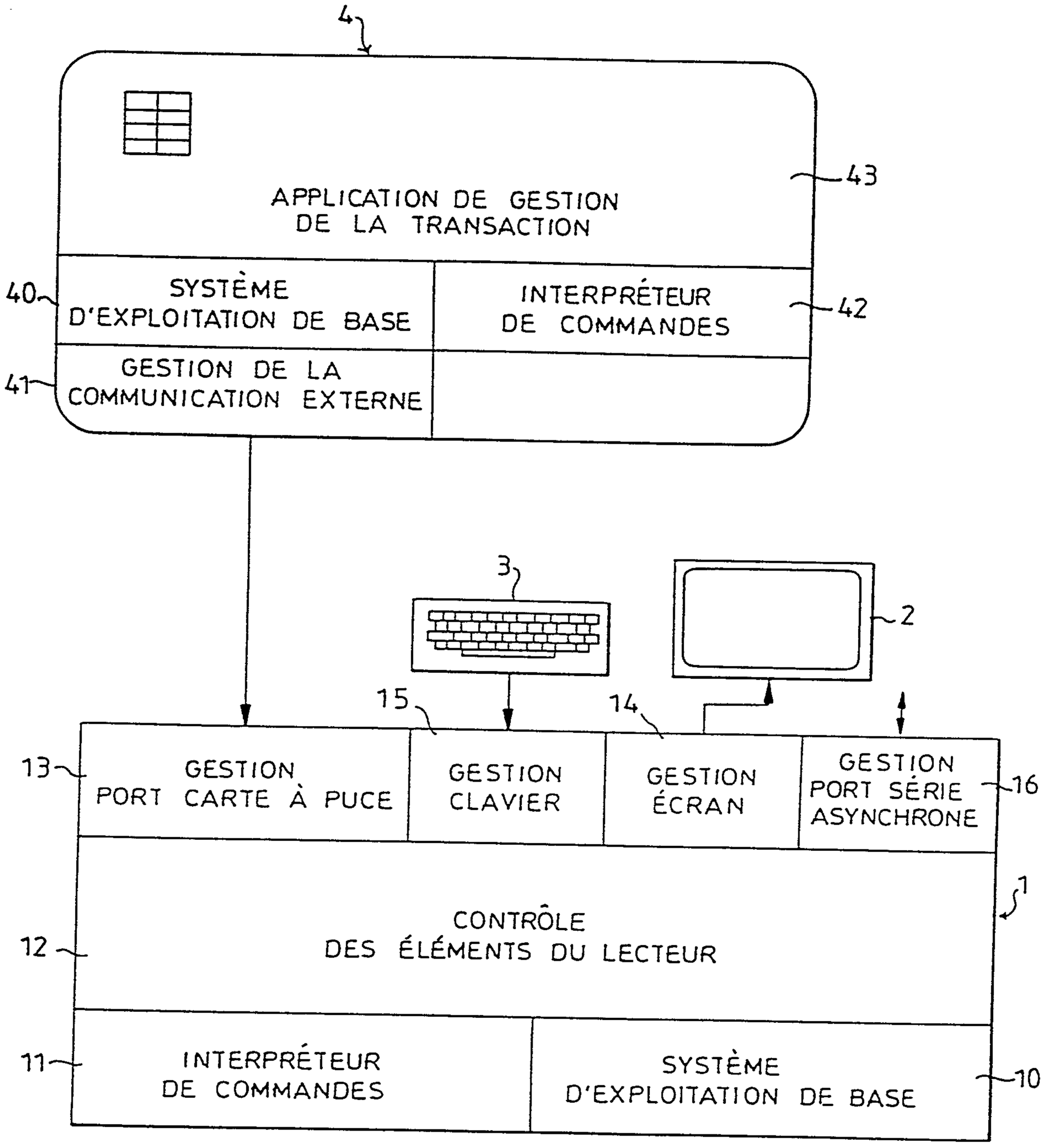
- demande de visualisation d'un message destiné à un opérateur,
- demande de sélection d'un menu,
- demande de saisie d'une grille,
- demande de visualisation d'une grille ou d'un champ,
- demande d'exécution d'une commande par les moyens de réception et de traitement de message carte du lecteur (1),
- demande d'enregistrement de fichier,
- demande d'authentification externe,
- demande de chiffrement,
- demande de déchiffrement,
- demande de signature d'un fichier,
- demande d'installation d'un programme,
- demande d'exécution d'un programme précédemment installé

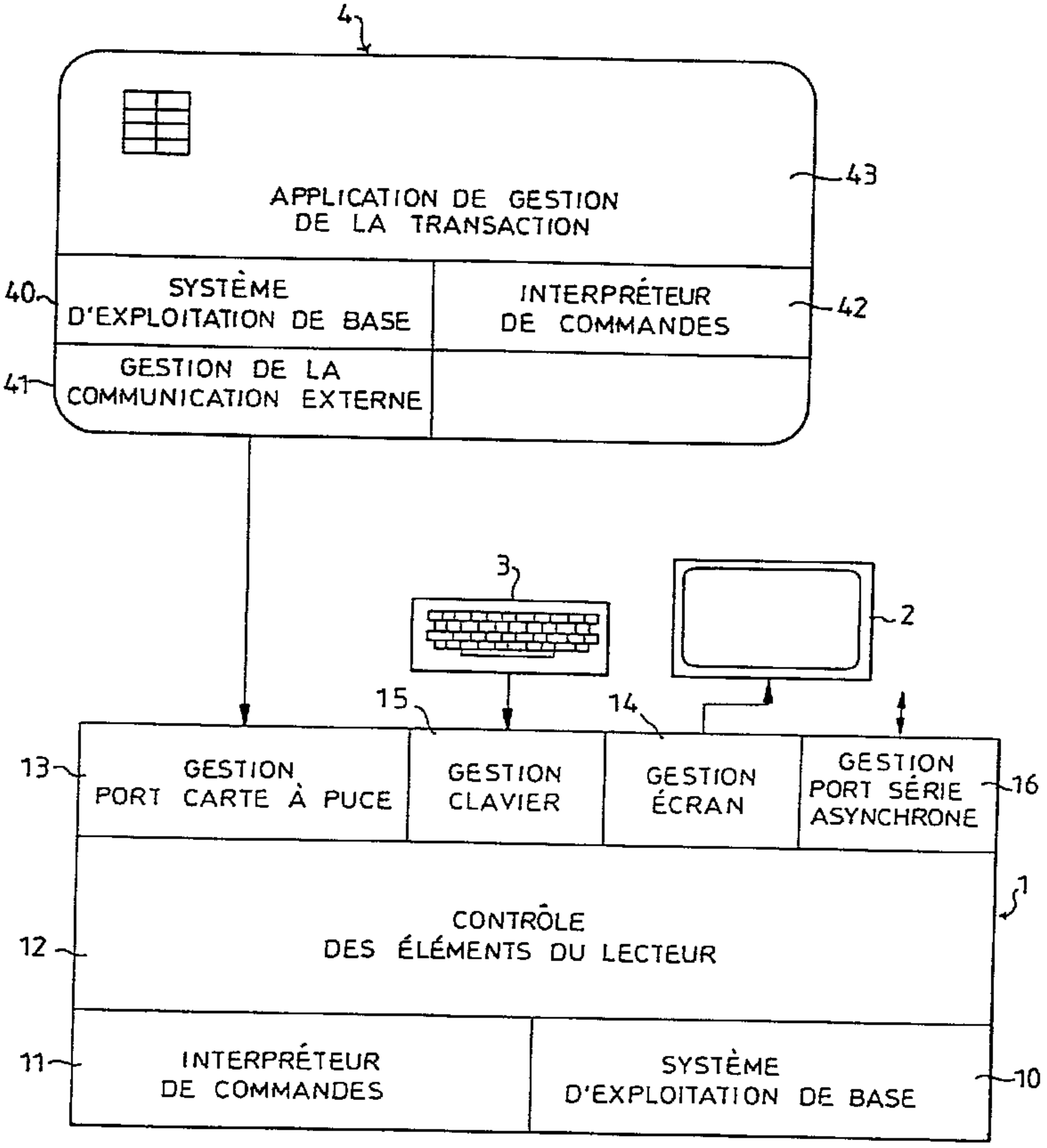
3. Système selon la revendication 1, caractérisé en ce que lesdits moyens d'élaboration de message de compte rendu dudit lecteur (1) élaborent des messages de compte rendu sur :

- une sélection d'un menu,
- une saisie d'un champ,
- une réponse à une demande d'exécution d'une commande par les moyens de réception et de traitement de message carte du lecteur (1),
- une insertion d'une carte à puce (4) dans le lecteur (1),
- un retrait d'une carte à puce (4) du lecteur (1),
- une inactivité du clavier,
- une authentification du lecteur (1)
- une demande de déchiffrement,
- un compte rendu d'installation,
- une demande d'une liaison asynchrone.

4. Système selon la revendication 1, caractérisé en ce que les moyens dudit lecteur (1) engendrant de manière alternative et répétitive une requête de mise à disposition d'un message carte et une déclaration de compte rendu associée à un message de compte rendu de la part du lecteur (1) élabore une requête de mise à disposition de message carte sous la forme d'un train numérique comportant plusieurs champs successifs dont un champ d'identification de commande et un champ de déclaration de la longueur du message carte attendu.

5. Système selon la revendication 1, caractérisé en ce que les moyens dudit lecteur (1) engendrant de manière alternative et répétitive une requête de mise à disposition d'un message carte et une déclaration de compte rendu associée à un message de compte rendu de la part du lecteur (1) élabore une déclaration de compte rendu sous la forme d'un train numérique comportant plusieurs champs successifs dont un champ d'identification de commande et un champ de déclaration de la longueur du message de compte rendu associé.


4
APPLICATION DE GESTION DE LA TRANSACTION
43
SYSTÈME D'EXPLOITATION DE BASE
40
INTERPRÉTEUR DE COMMANDES
42
GESTION DE LA COMMUNICATION EXTERNE
41
3
2
15
14
GESTION PORT CARTE À PUCE
13
GESTION CLAVIER
GESTION ÉCRAN
GESTION PORT SÉRIE ASYNCHRONE
16
CONTRÔLE DES ÉLÉMENTS DU LECTEUR
12
1
INTERPRÉTEUR DE COMMANDES
11
SYSTÈME D'EXPLOITATION DE BASE
10


4
APPLICATION DE GESTION DE LA TRANSACTION
43
40
SYSTÈME D'EXPLOITATION DE BASE
INTERPRÉTEUR DE COMMANDES
42
41
GESTION DE LA COMMUNICATION EXTERNE
3
2
15
14
13
GESTION PORT CARTE À PUCE
GESTION CLAVIER
GESTION ÉCRAN
GESTION PORT SÉRIE ASYNCHRONE
16
1
12
CONTRÔLE DES ÉLÉMENTS DU LECTEUR
11
INTERPRÉTEUR DE COMMANDES
SYSTÈME D'EXPLOITATION DE BASE
10