

12 DEMANDE DE BREVET D'INVENTION

A1

22 Date de dépôt : 12.11.15.

30 Priorité :

43 Date de mise à la disposition du public de la
demande : 19.05.17 Bulletin 17/20.

56 Liste des documents cités dans le rapport de
recherche préliminaire : Se reporter à la fin du
présent fascicule

60 Références à d'autres documents nationaux
apparentés :

○ Demande(s) d'extension :

71 Demandeur(s) : OBERTHUR TECHNOLOGIES
Société anonyme — FR.

72 Inventeur(s) : GILLES LESEIGNEUR et DUONG
BASTIEN.

73 Titulaire(s) : OBERTHUR TECHNOLOGIES Société
anonyme.

74 Mandataire(s) : CABINET BEAU DE LOMENIE.

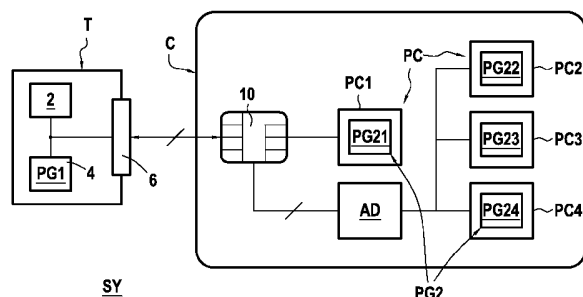
54 DISPOSITIF ELECTRONIQUE COMPRENANT UNE PLURALITE DE PUCES ELECTRONIQUES, ET TERMINAL
DE LECTURE APTE A COOPERER AVEC UN TEL DISPOSITIF.

57 L'invention concerne un dispositif électronique (C)
apte à coopérer avec un terminal de lecture (T), comprenant
une pluralité de puces (PC1-PC4), dans lequel :

- chaque puce (PC) est apte à commuter entre un premier mode dans lequel elle est apte à communiquer avec le terminal de lecture de façon bidirectionnelle et un deuxième mode dans lequel elle ne peut que recevoir une communication provenant du terminal de lecture ;

- chaque puce (PC) est apte à recevoir une commande de sélection reçue du terminal de lecture (T) pour sélectionner une unique puce (PC3) parmi les puces du dispositif ;

- lesdites puces (PC) étant configurées pour que, sur réception d'une commande de sélection de l'une des puces, la puce sélectionnée (PC3) commute dans le premier mode tandis que chaque autre puce (PC1, PC2, PC4) commute dans le deuxième mode.



5

Arrière-plan technologique

10 L'invention se rapporte au domaine des communications entre un dispositif électronique, tel qu'une carte à puce, et un terminal de lecture. L'invention porte plus particulièrement sur la communication entre un terminal de lecture et un tel dispositif comprenant une pluralité de puces électroniques distinctes.

15 L'invention trouve une application particulière dans une carte à puce (ou carte à microcircuit), conforme par exemple à la norme ISO 7816, comportant une pluralité de puces électronique distinctes, et également dans un lecteur adapté pour communiquer avec une telle carte à puce.

20 De manière générale, une carte à puce est conçue pour communiquer avec un dispositif externe à cette carte, autrement appelé terminal de lecture ou lecteur. Ces cartes permettent d'effectuer divers types de transactions, telles que des transactions de paiement, des transactions d'identification et/ou d'authentification du porteur etc. Les cartes à puce mettant en œuvre une ou plusieurs applications bancaires (carte de crédit, carte de débit etc.) sont par exemple aptes à communiquer avec des terminaux de paiement.

25 Dans les applications mises en œuvre aujourd'hui dans les cartes à puce, l'échange d'informations entre la carte à puce et le lecteur peut généralement se faire selon deux manières différentes : la communication par contact et celle dite sans contact. Dans le cas d'une communication par contact, les principaux protocoles utilisés définissent une communication entre deux – et seulement deux – entités, à savoir un dispositif de lecture
30 de carte à puce (un terminal de paiement par exemple) et une carte à puce. Plus spécifiquement, ces protocoles sont prévus pour permettre la communication entre le lecteur (agissant en tant que « maître »), d'une part, et une unique puce électronique de la carte à puce (agissant en tant qu'« esclave »), d'autre part.

35 Les protocoles de communication actuels (ISO 7816 par exemple) ne permettent pas à plusieurs puces distinctes d'une même carte à puce de dialoguer avec un lecteur lorsque lecteur et carte à puce coopèrent ensemble.

Cette contrainte pose aujourd'hui un problème majeur dans la mesure où les cartes à puce modernes sont de plus en plus complexes et peuvent à présent intégrer de multiples

puces afin d'enrichir l'expérience des utilisateurs ou de répondre à des besoins spécifiques. En effet, la mise en œuvre de différentes applications (bancaire, médicale, fidélité...) dans une même carte requière généralement des ressources matérielles qui ne peuvent être supportées sur une seule et même puce. Pour des raisons de confidentialité et de sécurité, il est également préférable de faire cohabiter plusieurs puces dans une même carte à puce afin de ne pas mettre en œuvre certaines applications sur une même puce.

Il est par exemple connu d'intégrer dans une même carte bancaire une première puce pour mettre en œuvre une transaction de paiement selon le standard ISO 7816 avec un lecteur externe, et une deuxième puce pour contrôler un afficheur ménagé dans la carte afin d'afficher des informations utiles à l'utilisateur.

Il devient cependant de plus en plus difficile d'enrichir les fonctionnalités d'une carte à puce tout en s'assurant que les protocoles de communication actuels sont respectés, notamment dans le cas particulier où plusieurs puces électroniques – dites « communicantes » – d'une même carte à puce sont présentes pour communiquer avec l'extérieur. On entend ici par « communicante », une puce apte à communiquer de façon bidirectionnelle avec le lecteur, c'est-à-dire en émission et en réception.

En effet, au sein d'une même carte à puce, seule une puce (agissant en tant qu'esclave) peut communiquer avec un lecteur (agissant en tant que maître) conformément aux protocoles actuels, les autres puces (agissant également comme esclaves) étant tout au plus capables de recevoir les informations entrantes dans la carte à puce en provenance du lecteur. En l'absence de message d'acquiescement, le lecteur n'a donc pas confirmation qu'une puce esclave non communicante de la carte à puce a bien reçu – et donc traite de façon adéquate – des données qui lui sont destinées.

Une approche consiste aujourd'hui à répéter plusieurs fois l'envoi de commandes par le lecteur afin d'augmenter les chances que ces commandes soient bien reçues et traitées par la puce esclave destinataire dans la carte à puce. Il est parfois également nécessaire de faire intervenir l'utilisateur afin de s'assurer qu'une commande est bien reçue (appui sur un bouton, vérification d'un affichage sur la carte...).

Il est donc aujourd'hui nécessaire d'optimiser la communication entre un terminal de lecture et une carte à puce (plus généralement un dispositif électronique) comprenant une pluralité de puces électroniques distinctes, de façon à ce que ledit terminal de lecture puisse s'assurer que chaque puce reçoit et traite correctement des informations dont elle est destinataire, et ce tout en respectant les protocoles de communication actuels (tel que ISO 7816 par exemple).

Objet et résumé

Un des buts de l'invention est de remédier aux insuffisances de l'état de la technique exposées ci-avant.

A cet effet, la présente invention concerne un dispositif électronique apte à coopérer avec un terminal de lecture, ledit dispositif comprenant une pluralité de puces distinctes, dans lequel :

- chaque puce est apte à commuter entre un premier mode de communication dans lequel elle est apte à communiquer avec le terminal de lecture de façon bidirectionnelle et un deuxième mode de communication dans lequel elle ne peut que recevoir une communication provenant du terminal de lecture ;
- chaque puce est apte à recevoir une commande de sélection reçue du terminal de lecture pour sélectionner une unique puce parmi lesdites puces du dispositif ;
- lesdites puces étant configurées de sorte que, sur réception d'une commande de sélection de l'une desdites puces, la puce sélectionnée commute dans le premier mode tandis que chaque autre puce commute dans le deuxième mode.

La présente invention permet d'optimiser la communication entre un terminal de lecture et une carte à puce (plus généralement un dispositif électronique) comprenant une pluralité de puces électroniques distinctes, de façon à ce que ledit terminal de lecture puisse s'assurer que chaque puce reçoit et traite correctement des informations dont elle est destinataire, et ce tout en respectant les protocoles de communication actuels (tel que ISO 7816 par exemple).

L'invention permet à chaque puce d'une carte à puce de dialoguer tour à tour avec un terminal de lecture. La sélection opérée par le terminal de lecture donne la capacité à une unique puce de ladite carte d'envoyer des informations au terminal de lecture, toutes les autres puces étant muettes afin de ne pas interférer. L'invention permet ainsi d'éviter toutes collisions éventuelles qui pourraient se produire si plusieurs puces d'une même carte tentaient de dialoguer en même temps avec le terminal de lecture (cette situation n'étant généralement pas bien supportée dans les protocoles de communication).

De manière avantageuse, un terminal de lecture peut en particulier sélectionner une puce à qui il s'apprête à envoyer une commande afin que la puce destinataire puisse envoyer en retour un message d'acquiescement attestant la bonne réception de la commande. L'invention permet ainsi de s'assurer avec certitude que des informations envoyées par le terminal de lecture ont bien été reçues par la puce destinataire.

Grâce à l'invention, il est possible de tirer meilleur profit d'une pluralité de puces électroniques présentes dans une même carte à puce, améliorant ainsi l'expérience de l'utilisateur et la fiabilité des communications.

Selon un mode de réalisation particulier, la commande de sélection comprend un identifiant de la puce sélectionnée, chaque puce étant apte à déterminer à partir dudit identifiant si elle doit commuter dans le premier ou le deuxième mode.

5 Selon un mode de réalisation particulier, ledit dispositif électronique est une carte à puce.

Selon un mode de réalisation particulier, ledit dispositif électronique est une carte à puce ISO 7816 apte à coopérer par contact avec le terminal de lecture.

Selon un mode de réalisation particulier, la commande de sélection est de type APDU.

10 Selon un mode de réalisation particulier, sur réception d'un signal RST (RESET) conforme à la norme ISO 7816 en provenance du terminal de lecture, les puces sont aptes à se configurer selon un état prédéterminé de sorte que, dans ledit état prédéterminé, l'une seulement desdites puces est dans le premier mode et chaque autre puce est dans le deuxième mode.

15 Selon un mode de réalisation particulier, l'une parmi lesdites puces est une puce dite principale et chaque autre puce parmi lesdites puces est une puce dite secondaire, la puce principale étant configurée pour répondre systématiquement par un message ATR à une commande RST reçue du terminal de lecture.

20 Selon un mode de réalisation particulier, sur réception de ladite commande RST émise par le terminal de lecture, chaque puce secondaire est configurée pour commuter dans le deuxième mode tandis que la puce principale est configurée pour commuter dans le premier mode. Dans cet exemple, la commande RST (appelée « Cold Reset » dans la norme ISO 7816) est accompagnée d'une coupure d'alimentation de la carte.

25 Selon un mode de réalisation particulier, sur réception de ladite commande RST émise par le terminal de lecture, les puces conservent leur état précédant la commande RST. Une commande RST est par exemple lancée lorsque la carte est sous tension. Dans la norme ISO 7816, cet état est appelé « Warm Reset ».

Corrélativement, l'invention concerne un terminal de lecture apte à coopérer avec un dispositif électronique comportant une pluralité de puces distinctes, dans lequel :

- 30
- chaque puce est apte à commuter entre un premier mode de communication dans lequel elle est apte à communiquer avec le terminal de lecture de façon bidirectionnelle et un deuxième mode de communication dans lequel elle ne peut que recevoir une communication provenant du terminal de lecture ;
 - le terminal de lecture est configuré pour envoyer au dispositif électronique une commande de sélection pour sélectionner une unique puce parmi lesdites puces
- 35
- du dispositif de sorte que la puce sélectionnée commute dans le premier mode tandis que chaque autre puce commute dans le deuxième mode.

Selon un mode de réalisation particulier, le terminal de lecture est configuré pour générer la commande de sélection à envoyer au dispositif électronique.

Selon un mode de réalisation particulier, ledit terminal de lecture est configuré pour inclure dans la commande de sélection un identifiant de la puce sélectionnée, de sorte
5 que chaque puce puisse déterminer à partir dudit identifiant si elle doit commuter dans le premier ou le deuxième mode.

La commande de sélection est par exemple une commande de type APDU.

La présente invention concerne également un système comprenant :

- un dispositif électronique tel que défini ci-avant ; et
- 10 - un terminal de lecture dudit dispositif électronique, tel que défini ci-avant.

La présente invention concerne également un signal émis par un terminal de lecture coopérant avec un dispositif électronique comprenant une pluralité de puces distinctes,

chaque puce dudit dispositif électronique étant apte à commuter entre un premier mode de communication dans lequel elle est apte à communiquer avec le terminal de lecture de façon
15 bidirectionnelle et un deuxième mode de communication dans lequel elle ne peut que recevoir une communication provenant du terminal de lecture ;

ledit signal comprenant une commande de sélection pour sélectionner une unique puce parmi lesdites puces dudit dispositif de sorte que la puce sélectionnée commute dans le premier mode tandis que chaque autre puce commute dans le deuxième mode.

20 L'invention propose par ailleurs un procédé de contrôle mise en œuvre par un dispositif électronique apte à coopérer avec un terminal de lecture, ledit dispositif comprenant une pluralité de puces distinctes, dans lequel :

- chaque puce est apte à commuter entre un premier mode de communication dans lequel elle est apte à communiquer avec le terminal de lecture de façon
25 bidirectionnelle et un deuxième mode de communication dans lequel elle ne peut que recevoir une communication provenant du terminal de lecture ;

ledit procédé comprenant les étapes suivantes :

- réception, par toutes les puces, d'une commande de sélection provenant du terminal de lecture pour sélectionner une unique puce parmi lesdites puces ;
- 30 - configuration desdites puces en réponse à ladite commande de sélection de sorte que :
 - o la puce sélectionnée commute dans le premier mode ; et
 - o chaque autre puce non sélectionnée commute dans le deuxième mode.

Selon un mode de réalisation particulier, le procédé comprend :

- 35 - détermination par chacune desdites puces, à partir d'un identifiant inclus dans la commande de sélection, de si ladite puce est sélectionnée ou non par la commande de sélection.

L'invention propose en outre un procédé de contrôle mis en œuvre par un terminal de lecture apte à coopérer avec un dispositif électronique comportant une pluralité de puces distinctes, dans lequel :

- 5 - chaque puce est apte à commuter entre un premier mode de communication dans lequel elle est apte à communiquer avec le terminal de lecture de façon bidirectionnelle et un deuxième mode de communication dans lequel elle ne peut que recevoir une communication provenant du terminal de lecture ;
 ledit procédé comprenant :
- 10 - envoi d'une commande de sélection pour sélectionner une unique puce parmi lesdites puces du dispositif de sorte que la puce sélectionnée commute dans le premier mode tandis que chaque autre puce non sélectionnée commute dans le deuxième mode.

À noter que les différents modes de réalisation définis ci-avant en relation avec le dispositif électronique, d'une part, et avec le terminal de lecture, d'autre part, ainsi que
15 les avantages associés à ces entités, s'appliquent par analogie aux procédés de contrôle respectifs définis ci-avant.

Dans un mode particulier de réalisation, les différentes étapes des procédés de contrôle sont déterminées par des instructions de programmes d'ordinateurs.

En conséquence, l'invention vise aussi un programme d'ordinateur sur un support
20 d'informations (ou support d'enregistrement), ce programme étant susceptible d'être mis en œuvre dans un dispositif électronique, dans un terminal de lecture, ou plus généralement dans un ordinateur, ce programme comportant des instructions adaptées à la mise en œuvre des étapes d'au moins l'un des procédés de contrôle tel que définis ci-dessus.

25 Ce programme peut utiliser n'importe quel langage de programmation, et être sous la forme de code source, code objet, ou de code intermédiaire entre code source et code objet, tel que dans une forme partiellement compilée, ou dans n'importe quelle autre forme souhaitable.

L'invention vise aussi un support d'informations (ou support d'enregistrement) lisible
30 par un ordinateur, et comportant des instructions d'un programme d'ordinateur tel que mentionné ci-dessus.

Le support d'informations peut être n'importe quelle entité ou dispositif capable de stocker le programme. Par exemple, le support peut comporter un moyen de stockage, tel qu'une ROM, par exemple un CD ROM ou une ROM de circuit microélectronique, ou
35 encore un moyen d'enregistrement magnétique, par exemple une disquette (floppy disc) ou un disque dur.

D'autre part, le support d'informations peut être un support transmissible tel qu'un signal électrique ou optique, qui peut être acheminé via un câble électrique ou optique, par radio ou par d'autres moyens. Le programme selon l'invention peut être en particulier téléchargé sur un réseau de type Internet.

5 Alternativement, le support d'informations peut être un circuit intégré dans lequel le programme est incorporé, le circuit étant adapté pour exécuter ou pour être utilisé dans l'exécution du procédé en question.

Brève description des dessins

10 D'autres caractéristiques et avantages de la présente invention ressortiront de la description faite ci-dessous, en référence aux dessins annexés qui en illustrent des exemples de réalisation dépourvus de tout caractère limitatif. Sur les figures:

- la figure 1 déjà décrite représente, de manière schématique, un système comportant une carte à puce et un terminal de lecture, conformément à un mode de réalisation particulier de l'invention ;
- 15 - la figure 2 représente schématiquement des modules mis en œuvre dans le terminal de lecture de la figure 1, conformément à un mode de réalisation particulier de l'invention ;
- la figure 3 représente schématiquement la structure de l'une des puces électroniques incluses dans la carte à puce illustrée en figure 1 ;
- 20 - la figure 4 représente schématiquement des modules mis en œuvre dans la puce électronique illustrée en figure 3, conformément à un mode de réalisation particulier de l'invention ;
- la figure 5 représente, sous forme d'un organigramme, les principales étapes de procédés de contrôle mis en œuvre respectivement par un terminal de lecture et par une carte à puce, conformément à un mode de réalisation particulier de l'invention ;
- 25 - les figures 6 et 7 représentent schématiquement l'état de configuration de puces électroniques d'une carte à puce, conformément à des modes de réalisation particulier ; et
- 30 - la figure 8 représente schématiquement la structure d'une commande de sélection, conformément à un mode de réalisation particulier.

Description détaillée de plusieurs modes de réalisation

35 Comme indiqué précédemment, l'invention se rapporte aux communications entre un dispositif électronique et un terminal de lecture. L'invention porte en particulier sur la

communication entre un terminal de lecture et un tel dispositif, lorsque ce dernier comprend une pluralité de puces électroniques distinctes.

5 Dans les exemples de réalisation qui suivent, le dispositif électronique est une carte à puce, celle-ci étant par exemple conforme au standard ISO 7816. On comprendra toutefois que l'invention n'est pas limitée à cette mise en œuvre particulière. Des dispositifs électroniques autres qu'une carte à puce peuvent notamment être envisagés.

10 Comme expliqué précédemment, la mise œuvre de plusieurs puces distinctes dans une carte à puce lorsque cette dernière coopère avec un terminal de lecture pose certaines difficultés. On entend dans cet exposé par puces distinctes, des puces électroniques comportant chacune leur propre interface de communication pour communiquer avec l'extérieur de la carte à puce. La disposition physique de ces puces peut varier selon le cas. En particulier, des puces distinctes peuvent être montées sur un même substrat, voir être englobées dans un même composant à l'intérieur de la carte à puce.

15 L'invention propose d'optimiser la communication entre une carte à puce dotée d'une pluralité de puces distinctes et un terminal de lecture de sorte que chaque puce de ladite carte puisse si nécessaire communiquer avec le terminal de lecture. Dans le présent exposé, et sauf indication contraire, on entend par « communiquer » le fait qu'une puce soit apte à communiquer de façon bidirectionnelle (en émission et en réception) avec une autre entité, à savoir le terminal de lecture dans les exemples qui suivent.

20 L'invention, selon ses différents modes de réalisation, met ainsi en œuvre une carte à puce comportant une pluralité de puces distinctes, chacun d'elle étant apte à commuter entre un mode dit « communicant » dans lequel elle peut communiquer (de façon bidirectionnelle) avec le terminal de lecture, et un mode dit « d'écoute » dans lequel elle peut seulement recevoir une communication provenant du terminal de lecture. Le terminal de lecture est apte à sélectionner une unique puce parmi celles de la carte à puce de sorte que seule la puce sélectionnée fonctionne en mode « communicant », toutes les autres puces non sélectionnées fonctionnant en mode « d'écoute ». Il est ainsi possible d'éviter toute collision entre des données émises en même temps par des puces distinctes à destination du terminal de lecture.

30 Sauf indications contraires, les éléments communs ou analogues à plusieurs figures portent les mêmes signes de référence et présentent des caractéristiques identiques ou analogues, de sorte que ces éléments communs ne sont généralement pas à nouveau décrits par souci de simplicité.

35 La **figure 1** représente schématiquement la structure d'un terminal de lecture T (nommé par la suite « terminal ») et d'un dispositif électronique C prenant ici la forme

d'une carte à puce, conformément à un mode de réalisation particulier. Le terminal T et la carte à puce C sont aptes à coopérer ensemble pour former un système SY.

Dans l'exemple envisagé ici, la carte à puce C et le terminal T sont configurés pour coopérer ensemble selon le protocole ISO 7816.

5 Dans la suite de cet exposé, on comprendra que certains éléments généralement présents dans une carte à puce, ou dans un lecteur d'une telle carte, ont été volontairement omis car ils ne sont pas nécessaires à la compréhension de la présente invention.

10 Plus spécifiquement, le terminal T comprend ici un processeur 2, une mémoire non volatile 4 et un connecteur 6.

La mémoire 4 est une mémoire non volatile réinscriptible ou une mémoire morte (ROM), cette mémoire constituant un support d'enregistrement (ou support d'informations) conforme à un mode de réalisation particulier, lisible par le terminal T, et sur lequel est enregistré un programme d'ordinateur PG1 conforme à un mode de réalisation particulier. Ce programme d'ordinateur PG1 comporte des instructions pour l'exécution des étapes d'un procédé de contrôle selon un mode de réalisation particulier.

Le connecteur 6 est configuré de sorte à pouvoir être couplé de façon amovible avec des contacts 10 disposés sur la carte C, comme expliqué ci-après.

20 Comme représenté en **figure 2**, le processeur 2 piloté par le programme d'ordinateur PG1 met ici en œuvre un module de génération de commande 20 et un module d'envoi 22. Le module de génération de commande 20 est apte à générer des commandes (APDU dans cet exemple) à destination de la carte à puce C. Comme expliqué ci-après, le module de génération de commande est en particulier apte à générer des commandes de sélection. Le module d'envoi 22 est par ailleurs apte à envoyer chaque commande générée vers la carte C lorsque celle-ci coopère par contact avec le terminal T.

25 Comme illustré en **figure 1**, la carte à puce C comprend des contacts 10, un module AD, et une pluralité de puces électroniques distinctes, à savoir quatre puces distinctes PC1, PC2, PC3 et PC4 (notées collectivement PC) dans cet exemple. Le nombre de puces PC peut naturellement être adapté selon le cas d'usage, étant entendu que le nombre de puces PC est au moins de 2 dans la carte C.

30 Comme déjà indiqué, les contacts 10 sont adaptés pour pouvoir être couplés avec le connecteur 6 du terminal T.

35 Dans cet exemple de réalisation, un module d'adaptation AD fait l'interface entre les contacts 10 de la carte à puce C et les puces électroniques PC2, PC3 et PC4. Ce module d'adaptation AD est un élément optionnel qui permet dans cet exemple d'adapter la tension délivrée à chacune des puces PC2, PC3 et PC4 à partir de la tension appliquée par le terminal T via les contacts 10.

La fonction et la nature de chaque puce peuvent également varier selon le cas d'espèce. Chaque puce peut être configurée pour mettre en œuvre au moins une application spécifique (bancaire, d'authentification, de fidélité etc.).

Conformément à ce mode de réalisation, chacune des puces électroniques PC est
5 apte à commuter entre un premier mode de communication M1 (dit « mode communicant » ou bidirectionnel) et un deuxième mode de communication M2 (dit « mode d'écoute »). Chaque puce PC fonctionnant en mode communicant M1 est apte à communiquer avec le terminal T de façon bidirectionnelle. Autrement dit, la puce PC concernée est capable de recevoir des données provenant du terminal T et d'envoyer des
10 données au terminal T. Par ailleurs, chaque puce PC fonctionnant en mode d'écoute M2 ne peut que recevoir une communication provenant du terminal T. Autrement dit, en mode d'écoute M2, la communication entre le terminal T et la puce PC concernée n'est possible que depuis le terminal T vers la puce PC en question.

Aussi, chaque puce PC est au moins apte à recevoir des commandes provenant du
15 terminal T, que le mode de communication utilisée soit M1 ou M2.

La **figure 3** représente schématiquement la structure de la puce PC1. On supposera ici que les autres puces PC2, PC3 et PC4 présentent chacune une structure analogue à la puce PC1 et ne seront donc pas décrites en détail par souci de simplicité.

Plus spécifiquement, la puce PC1 comprend un processeur 30, une interface de
20 communication 32 et une mémoire non volatile 34.

La puce PC1 est apte, à partir de l'interface de communication 32, à communiquer via les contacts 10 avec l'extérieur de la carte à puce C, plus particulièrement avec le terminal T dans cet exemple.

La mémoire 34 est une mémoire non volatile réinscriptible ou une mémoire morte
25 (ROM), cette mémoire constituant un support d'enregistrement (ou support d'informations) conforme à un mode de réalisation particulier, lisible par la puce PC1, et sur lequel est enregistré un programme d'ordinateur PG21 conforme à un mode de réalisation particulier.

De façon analogue, les puces PC2, PC3 et PC4 comportent chacune dans une
30 mémoire (non représentée) un programme d'ordinateur PG22, PG23 et PG24, respectivement. Les programmes d'ordinateur PG21-PG24 comportent ainsi collectivement des instructions pour l'exécution des étapes d'un procédé de contrôle de la carte à puce C selon un mode de réalisation particulier.

Comme représenté en **figure 4**, le processeur 30 piloté par le programme
35 d'ordinateur PG21, met ici en œuvre un module de traitement 40 et un module de configuration 42. On supposera de la même manière que le processeur de chaque autre

puce PC2-PC4 met en œuvre des modules analogues à ceux mentionnés ci-dessus pour le processeur 30 de PC1.

5 Plus spécifiquement, le module de traitement 40 est apte à traiter des commandes du terminal T. Dans le mode de réalisation décrit ici, le module de traitement 40 est en particulier configuré pour recevoir et traiter des commandes de sélection susceptibles d'être envoyées par le terminal T comme expliqué ci-après. Par ailleurs, le module de configuration 42 est apte à commuter de façon appropriée la puce PC1 dans le mode communicant M1 ou dans le mode d'écoute M2.

10 Conformément à ce mode de réalisation particulier, chaque puce PC est configurée de sorte que, sur réception d'une commande de sélection envoyée par le terminal T pour sélectionner une unique puce PC dans la carte C, la puce sélectionnée PC commute dans le mode communicant M1 tandis que chaque autre puce PC non sélectionnée commute dans le mode d'écoute M2.

15 Un mode de réalisation particulier est à présent décrit en référence aux **figures 5, 6 et 7**. Plus précisément, le terminal T met en œuvre un procédé de contrôle en exécutant le programme d'ordinateur PG1. De même, la carte à puce C met en œuvre un procédé de contrôle en exécutant les programmes d'ordinateur PG21 à PG24 (formant collectivement un programme d'ordinateur PG2).

20 On supposera dans ce mode de réalisation que le terminal de lecture T est couplé avec la carte à puce C.

On suppose par ailleurs que la carte à puce C se trouve dans un état initial illustré en **figure 6**, dans lequel :

- 25 - la puce PC1 est en mode communicant M1 de sorte qu'elle est apte à recevoir (RX) des données provenant du terminal T et à envoyer (TX) des données au terminal (mode de communication bidirectionnel) ; et
- les puces PC2, PC3 et PC4 sont chacune en mode d'écoute M2 de sorte que chacune d'elles ne peut que recevoir une communication du terminal T (mode unidirectionnel depuis le terminal T vers chaque puce PC concernée).

30 Comme indiqué précédemment, le terminal T et la carte à puce C communiquent ici selon le protocole ISO 7816.

Au cours d'une étape A2, le terminal T envoie un message d'initialisation RST (de type RESET). Ce message RST est reçu (B2) par toutes les puces PC1 à PC4.

35 Le terminal T est l'entité qui initie l'interaction avec la carte à puce C ; le terminal T agit par conséquent comme maître dans cette transaction tandis que chacune des puce PC de la carte à puce C agit en tant qu'esclave.

Dans le mode de réalisation décrit ici, la puce PC1 est par défaut la puce esclave répondant au message d'initialisation RST. A ce titre, la puce PC1 est considérée comme

puce principale dans le sens où elle est en charge d'envoyer le message de réponse ATR au terminal T. Les autres puces PC2-PC4 agissent en tant que puce esclave secondaire dans la mesure où, par défaut, elles sont en mode d'écoute M2 et à ce titre ne sont pas aptes à envoyer un ATR en réponse au message RST du terminal T. On comprendra toutefois que d'autres mises en œuvre sont possibles dans le cadre de l'invention.

Etant l'unique puce PC en mode communication M1, la puce PC1 est la seule à répondre au RST en envoyant (B4) un message ATR (Answer-to-Reset) au terminal T. Les puces PC2 à PC4 restent muettes (elles n'envoient aucun message en retour au terminal T).

Une fois le message ATR reçu (A4), le terminal T envoie la ou les commandes APDU nécessaires pour réaliser la transaction (ou l'opération) désirée avec la carte à puce C.

Dans cet exemple particulier, on suppose que le terminal T a besoin de communiquer avec la puce électronique PC3. Cette dernière étant à ce stade en mode d'écoute M2, elle n'est pas apte à émettre à destination du terminal T.

Pour ce faire, le module de génération 20 du terminal T génère (A6) une commande de sélection CMD1 pour sélectionner la puce PC3 – et seulement la puce PC3 – parmi les puces PC de la carte à puce C. Dans un exemple de réalisation particulier, cette commande CMD1 comprend un identifiant ID3 de la puce PC3 sélectionnée, cet identifiant étant inclus par le module de génération 20 lors de la génération A6.

La commande de sélection CMD1 est par exemple une commande de type APDU. Elle présente par exemple la structure représentée en **figure 8**. Cette figure représente une commande de sélection se présentant sous la forme d'une trame comportant les champs suivants :

- CLA : la classe d'instruction indiquant le type de la commande ;
- INS : le code d'instruction indiquant le code de commande ;
- P1 et P2 : les paramètres d'instructions de la commande ;
- Lc : définit le nombre d'octets envoyés par la commande ;
- Data : nombre d'octets ;
- Le : le nombre d'octets maximum attendus dans la réponse.

Dans cette mise en œuvre particulière, le champ P2 comporte par exemple l'identifiant (ou index) ID3 désignant la puce PC3 comme la puce esclave sélectionnée.

Selon un exemple particulier, le champ P2 comprend un code identifiant la puce PC3 en tant que puce à sélectionner.

Le terminal T envoie (A8) ensuite, à l'aide de son module d'envoi 22, la commande de sélection CMD1 à la carte à puce C.

Chacune des puces PC1, PC2, PC3 et PC4 reçoit (B8) dans cet exemple la commande de sélection CMD1. Le module de traitement 40 de chaque puce PC analyse (B10) alors la

commande de sélection CMD1 et détermine (B10), à partir de cette commande (plus particulièrement ici à l'aide de l'identifiant ID3), si la puce PC concernée est sélectionnée ou non. Dans cet exemple, chaque puce PC détectant que l'identifiant ID3 ne correspondant pas à son propre identifiant en déduit qu'elle n'est pas sélectionnée.

- 5 Au cours de l'étape de configuration B12, les puces PC se configurent de sorte que :
- la puce PC sélectionnée (la puce PC3 dans cet exemple) par la commande CMD1 commute (B12) en mode communicant M1 de sorte à pouvoir communiquer de façon bidirectionnelle avec le terminal T ;
 - toutes les autres puces PC non sélectionnées (PC1, PC2 et PC4 dans cet
- 10 exemple) commutent (B12) en mode d'écoute M2 de sorte qu'elles ne puissent plus que recevoir les commandes émanant du terminal T.

On comprend ici par « commuter » le fait qu'une puce se configure dans l'un des modes de communication M1 et M2 considérés, étant entendu qu'aucun changement de mode n'est nécessaire si la puce était déjà dans le mode approprié au moment de la

15 commutation.

La **figure 7** représente schématiquement la configuration des puces PC une fois la configuration B12 réalisée.

Au cours de l'étape d'envoi B14 (**figure 5**), la puce PC sélectionnée (PC3 dans cet exemple) envoie un octet de procédure OP (« procedure byte » en anglais), indiquant qu'elle a bien pris en compte la commande de sélection CMD1. Cet octet de procédure OP peut être par exemple un octet d'acquiescement, un code de réponse (« status word » en anglais) ou encore un code d'erreur.

20

Après réception (A14) de cet octet de procédure OP, le terminal T peut le cas échéant envoyer d'autres informations complémentaires afin de réaliser une opération donnée avec la puce PC sélectionnée.

25

On notera que le terminal T peut si besoin sélectionner ultérieurement une autre puce PC afin de rendre à son tour cette dernière apte à répondre aux commandes du terminal T. Pour ce faire, le terminal T envoie (A16) une autre commande de sélection (notée cette fois CMD2) afin de sélectionner la puce PC appropriée, comme illustré en

30 **figure 5.**

Dans un exemple de réalisation particulier, les puces PC se configurent dans l'état initial prédéterminé représenté en **figure 6** sur réception d'un signal RST conforme à la norme ISO 7816 envoyé par le terminal T. Cet état prédéterminé peut être adapté selon le cas d'usage, étant entendu que, dans cet état prédéterminé, une unique puce PC commute dans le premier mode M1 et chaque autre puce PC commute dans le deuxième mode M2.

35

Dans le mode de réalisation décrit en référence à la **figure 5**, le terminal de lecture T est apte à générer la commande de sélection CMD1 envoyée à l'étape d'envoi A8. On comprendra toutefois qu'il n'est pas obligatoire que ce soit le terminal de lecture T qui génère la commande de sélection au sens de l'invention. Selon un exemple particulier, le terminal de lecture T reçoit cette commande de sélection d'un dispositif externe, depuis un système bancaire par exemple. Le terminal de lecture T est alors configuré pour transmettre à la carte à puce C la commande de sélection reçue de l'extérieur.

Dans un exemple particulier, le terminal de lecture T réalise une transaction bancaire en coopération avec la carte à puce C. Un serveur bancaire envoie par exemple à la fin de la transaction une pluralité de commandes au terminal de lecture T, notamment une commande de sélection au sens de l'invention. Pour ce faire, le terminal de lecture T doit être connecté au serveur bancaire en question. Dans cet exemple particulier, le terminal de lecture T n'est pas capable de comprendre cette commande de sélection. Le terminal de lecture T est configuré pour transmettre cette commande de sélection à la carte à puce C. La génération de la commande de sélection n'est donc pas réalisée par le terminal de lecture T dans ce cas particulier.

La présente invention peut trouver différentes applications.

Selon une application particulière, la présente invention est utilisée lors de la personnalisation de la carte à puce C. Plus spécifiquement, lors d'une personnalisation de la carte C, le terminal de lecture T est par exemple configuré pour envoyer des signaux à divers puces électroniques présentes dans la carte à puce. Le terminal de lecture envoie des commandes de sélection afin de sélectionner tour à tour chaque puce avec laquelle un dialogue est nécessaire. Une fois sélectionnée, chaque puce concernée peut ainsi répondre de façon appropriée au terminal de lecture, ce qui permet à ce dernier de s'assurer que des données envoyées lors du processus de personnalisation ont bien été reçues par la puce destinataire. Dans cette application particulière, l'invention permet d'améliorer significativement la personnalisation d'une carte à puce.

Selon une application particulière, la présente invention est utilisée en cours d'utilisation de la carte à puce par un utilisateur. Dans un exemple particulier, la carte à puce C comprend un afficheur contrôlé par une puce spécifique (notée ici PC2 par exemple) de la carte C. L'afficheur est apte, sous contrôle de la puce PC2, à afficher des informations utiles à l'utilisateur. Le terminal de lecture T est par exemple configuré pour envoyer une commande d'affichage à la puce PC2 de la carte C afin de commander l'affichage sur l'afficheur de données, telles qu'un solde de compte ou toutes autres informations (bancaires...) appropriées. Dans cet exemple particulier, le terminal de lecture est apte à envoyer une commande de sélection afin de sélectionner la puce PC2

contrôlant l'afficheur afin de s'assurer que ladite puce PC2 a bien pris en compte une commande d'affichage du terminal de lecture.

5 Dans un exemple particulier, la carte à puce C comprend un capteur biométrique contrôlé par une puce spécifique (notée ici PC3 par exemple) de la carte C. Le capteur est apte, sous contrôle de la puce PC3, à collecter des informations biométriques de l'utilisateur. Le terminal de lecture T est par exemple configuré pour envoyer une commande de récupération des données à la puce PC3 de la carte C afin de commander l'activation du capteur biométrique. Ces données peuvent ensuite être utilisées par la puce PC1 afin d'authentifier le porteur de la carte à puce.

10 L'invention permet d'optimiser la communication entre un terminal de lecture et une carte à puce (plus généralement un dispositif électronique) comportant une pluralité de puces électroniques distinctes, tout en respectant les protocoles de communications actuels (tel que ISO 7816 par exemple).

15 L'invention permet à chaque puce d'une carte à puce de dialoguer tour à tour avec un terminal de lecture. La sélection opérée par le terminal de lecture donne la capacité à une unique puce de ladite carte d'envoyer des informations au terminal de lecture, toutes les autres puces étant muettes afin de ne pas interférer. L'invention permet ainsi d'éviter toutes collisions éventuelles qui pourraient se produire si plusieurs puces d'une même carte tentaient de dialoguer en même temps avec le terminal de lecture (cette situation n'étant généralement pas bien supportée dans les protocoles de communication).

20 De manière avantageuse, un terminal de lecture peut en particulier sélectionner une puce à qui il s'apprête à envoyer une commande afin que la puce destinataire puisse envoyer en retour un message d'acquiescement attestant la bonne réception de la commande. L'invention permet ainsi de s'assurer avec certitude que des informations envoyées par le terminal de lecture ont bien été reçues par la puce destinataire.

25 Grâce à l'invention, il est possible de tirer meilleur profit d'une pluralité de puces électroniques présentes dans une même carte à puce, améliorant ainsi l'expérience de l'utilisateur et la fiabilité des communications.

30 Un homme du métier comprendra que les modes de réalisation et variantes décrits ci-avant ne constituent que des exemples non limitatifs de mise en œuvre de l'invention. En particulier, l'homme du métier pourra envisager une quelconque adaptation ou combinaison des modes de réalisation et variantes décrits ci-avant afin de répondre à un besoin bien particulier.

35 Selon un mode de réalisation, l'invention est mise en œuvre au moyen de composants logiciels et/ou matériels. Dans cette optique, le terme « module » employé dans le présent exposé peut correspondre aussi bien à un composant logiciel, qu'à un composant matériel ou à un ensemble de composants matériels et logiciels.

REVENDICATIONS

- 5 1. Dispositif électronique (C) apte à coopérer avec un terminal de lecture (T), ledit dispositif comprenant une pluralité de puces distinctes (PC1-PC4), caractérisé en ce que :
- 10 - chaque puce (PC) est apte à commuter entre un premier mode de communication (M1) dans lequel elle est apte à communiquer avec le terminal de lecture de façon bidirectionnelle et un deuxième mode de communication (M2) dans lequel elle ne peut que recevoir une communication provenant du terminal de lecture ;
- 15 - chaque puce (PC) est apte à recevoir une commande de sélection (CMD1) reçue du terminal de lecture (T) pour sélectionner une unique puce (PC3) parmi lesdites puces du dispositif ;
- 20 - lesdites puces (PC) étant configurées de sorte que, sur réception d'une commande de sélection (CMD1) de l'une desdites puces, la puce sélectionnée (PC3) commute dans le premier mode (M1) tandis que chaque autre puce (PC1, PC2, PC4) commute dans le deuxième mode (M2).
- 25 2. Dispositif électronique selon la revendication 1, la commande de sélection (CMD1) comprenant un identifiant (ID3) de la puce sélectionnée (PC3), chaque puce (PC) étant apte à déterminer à partir dudit identifiant si elle doit commuter dans le premier ou le deuxième mode.
- 30 3. Dispositif électronique selon la revendication 1 ou 2, ledit dispositif électronique (C) étant une carte à puce.
- 35 4. Dispositif électronique selon la revendication 3, ledit dispositif électronique étant une carte à puce (C) ISO 7816 apte à coopérer par contact avec le terminal de lecture (T).
5. Dispositif électronique selon la revendication 4, dans lequel la commande de sélection (CMD1) est de type APDU.
6. Dispositif électronique selon la revendication 4, dans lequel, sur réception d'un signal RST conforme à la norme ISO 7816 en provenance du terminal de lecture (T), les puces (PC) sont aptes à se configurer selon un état prédéterminé de sorte que, dans ledit

état prédéterminé, l'une seulement desdites puces est dans le premier mode (M1) et chaque autre puce (PC2-PC4) est dans le deuxième mode (M2).

5 7. Dispositif électronique selon l'une quelconque des revendications 1 à 6, dans lequel l'une (PC1) parmi lesdites puces (PC) est une puce dite principale et chaque autre puce (PC2-PC4) parmi lesdites puces est une puce dite secondaire,

la puce principale étant configurée pour répondre systématiquement par un message ATR à une commande RST reçue du terminal de lecture.

10 8. Dispositif électronique selon la revendication 7, dans lequel, sur réception de ladite commande RST émise par le terminal de lecture (T), chaque puce secondaire (PC2-PC4) est configurée pour commuter dans le deuxième mode (M2) tandis que la puce principale est configurée pour commuter dans le premier mode (M1).

15 9. Terminal de lecture (T) apte à coopérer avec un dispositif électronique (C) comportant une pluralité de puces distinctes (PC), caractérisé en ce que :

- chaque puce (PC) est apte à commuter entre un premier mode de communication (M1) dans lequel elle est apte à communiquer avec le terminal de lecture de façon bidirectionnelle et un deuxième mode de communication (M2)
20 dans lequel elle ne peut que recevoir une communication provenant du terminal de lecture ;
- le terminal de lecture est configuré pour envoyer au dispositif électronique (C) une commande de sélection (CMD1) pour sélectionner une unique puce (PC3) parmi lesdites puces dudit dispositif de sorte que la puce sélectionnée (PC3)
25 commute dans le premier mode (M1) tandis que chaque autre puce (PC1, PC2, PC4) commute dans le deuxième mode (M2).

30 10. Terminal de lecture selon la revendication 9, dans lequel ledit terminal de lecture est configuré pour générer la commande de sélection (CMD1) à envoyer au dispositif électronique (C).

35 11. Terminal de lecture selon la revendication 9 ou 10, dans lequel ledit terminal de lecture est configuré pour inclure dans la commande de sélection (CMD1) un identifiant (ID3) de la puce sélectionnée, de sorte que chaque puce (PC) puisse déterminer à partir dudit identifiant si elle doit commuter dans le premier ou le deuxième mode.

12. Système comprenant :

- un dispositif électronique (C) selon l'une quelconque des revendications 1 à 8 ; et
- un terminal de lecture (T) dudit dispositif électronique selon l'une quelconque des revendications 9 à 11.

5 13. Signal émis par un terminal de lecture (T) coopérant avec un dispositif électronique (C) comprenant une pluralité de puces distinctes (PC1-PC4),

chaque puce (PC) dudit dispositif électronique étant apte à commuter entre un premier mode de communication (M1) dans lequel elle est apte à communiquer avec le terminal de lecture de façon bidirectionnelle et un deuxième mode de communication (M2) dans
10 lequel elle ne peut que recevoir une communication provenant du terminal de lecture ;

ledit signal comprenant une commande de sélection (CMD1) pour sélectionner une unique puce (PC3) parmi lesdites puces dudit dispositif de sorte que la puce sélectionnée (PC3) commute dans le premier mode (M1) tandis que chaque autre puce (PC1, PC2, PC4) commute dans le deuxième mode (M2).

15

14. Procédé de contrôle mise en œuvre par un dispositif électronique (C) apte à coopérer avec un terminal de lecture (T), ledit dispositif comprenant une pluralité de puces (PC1-PC4) distinctes, caractérisé en ce que :

- chaque puce (PC) est apte à commuter entre un premier mode de communication (M1) dans lequel elle est apte à communiquer avec le terminal de lecture de façon bidirectionnelle et un deuxième mode de communication (M2) dans lequel elle ne peut que recevoir une communication provenant du terminal de lecture ;

ledit procédé comprenant les étapes suivantes :

- 25 - réception (B8), par toutes les puces (PC), d'une commande de sélection (CMD1) provenant du terminal de lecture (T) pour sélectionner une unique puce (PC3) parmi lesdites puces ;
- configuration desdites puces (PC) en réponse à ladite commande de sélection de sorte que :
 - 30 o la puce sélectionnée (PC3) commute dans le premier mode (M1) ; et
 - o chaque autre puce non sélectionnée (PC1, PC2, PC4) commute dans le deuxième mode.

30

15. Procédé de contrôle selon la revendication 14, comprenant :

- 35 - détermination (B10) par chacune desdites puces, à partir d'un identifiant (ID3) inclus dans la commande de sélection (CMD3), de si ladite puce (PC) est sélectionnée ou non par la commande de sélection.

16. Procédé de contrôle mis en œuvre par un terminal de lecture (T) apte à coopérer avec un dispositif électronique (C) comportant une pluralité de puces (PC1-PC4) distinctes, caractérisé en ce que :

- 5 - chaque puce (PC) est apte à commuter entre un premier mode de communication (M1) dans lequel elle est apte à communiquer avec le terminal de lecture de façon bidirectionnelle et un deuxième mode de communication (M2) dans lequel elle ne peut que recevoir une communication provenant du terminal de lecture ;

10 ledit procédé comprenant :

- envoi (A8) d'une commande de sélection (CMD1) pour sélectionner une unique puce (PC3) parmi lesdites puces du dispositif de sorte que la puce sélectionnée (PC3) commute dans le premier mode (M1) tandis que chaque autre puce non sélectionnée (PC1, PC2, PC4) commute dans le deuxième mode.

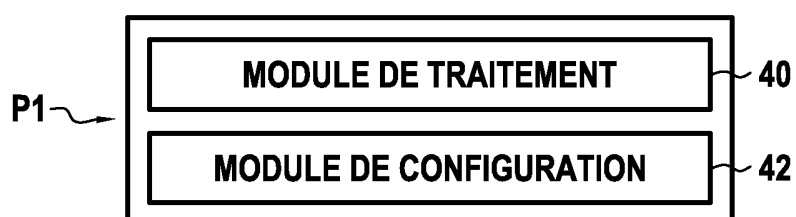
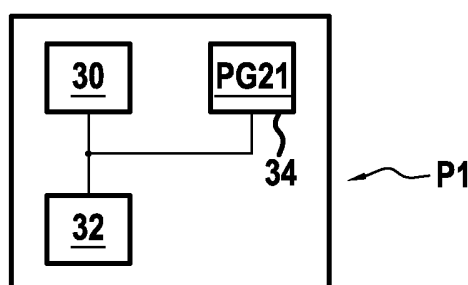
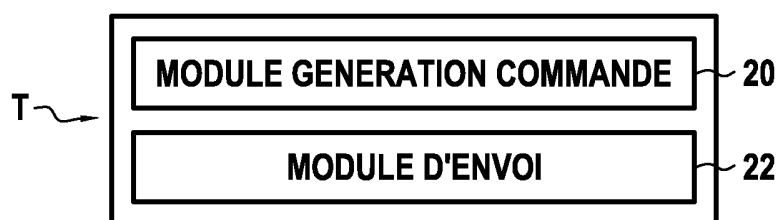
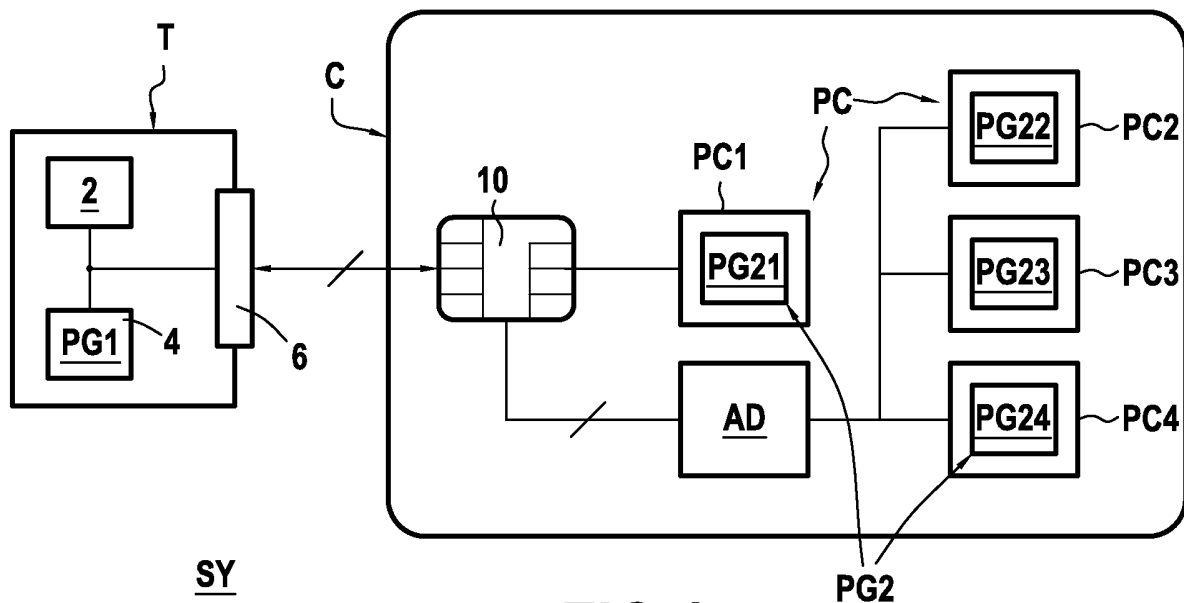
15

17. Programme d'ordinateur (PG1 ; PG21-PG24) comportant des instructions pour l'exécution des étapes d'un procédé selon l'une quelconque des revendications 14 à 16 lorsque ledit programme est exécuté par un ordinateur.

20

18. Support d'enregistrement (4 ; 34) lisible par un ordinateur sur lequel est enregistré un programme d'ordinateur (PG1 ; PG21-P24) comprenant des instructions pour l'exécution des étapes d'un procédé selon l'une quelconque des revendications 14 à 16.

1/2



2/2

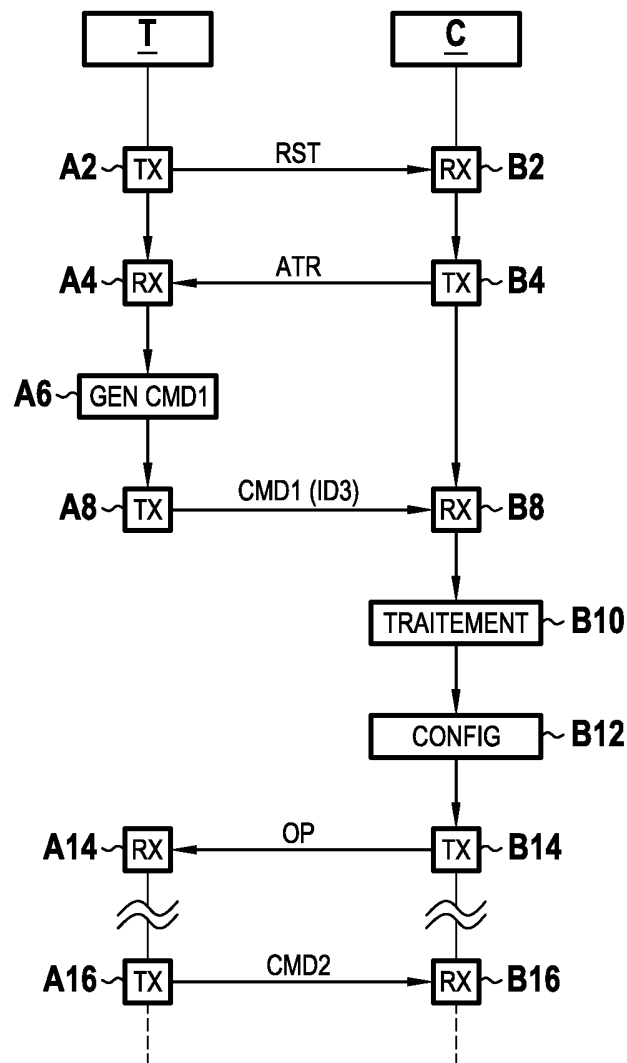


FIG.5

FIG.6

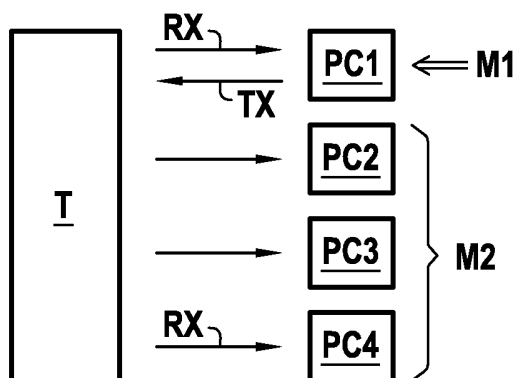
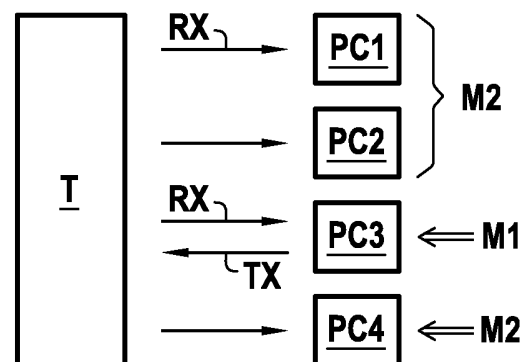


FIG.7



Commande APDU						
CLA	INS	P1	P2	Lc	Data	Le
1 octet	1 octet	1 octet	1 octet	0,1 ou 3 octets	n octets	0,1 ou 3 octets

FIG.8



RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications
déposées avant le commencement de la recherche

N° d'enregistrement
national

FA 819509
FR 1560810

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	US 5 838 059 A (INOUE MASAYUKI [JP] ET AL) 17 novembre 1998 (1998-11-17) * abrégé * * colonne 3, ligne 66 - colonne 8, ligne 52; revendications 1-10; figures 1, 4-9 * -----	1-18	G06K19/07 G06K7/00
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			G06K
Date d'achèvement de la recherche 30 juin 2016		Examineur Savvides, George	
CATÉGORIE DES DOCUMENTS CITÉS X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : arrière-plan technologique O : divulgation non-écrite P : document intercalaire		T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant	

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE**RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1560810 FA 819509**

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.

Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du **30-06-2016**

Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 5838059 A	17-11-1998	CN 1165354 A	19-11-1997
		DE 69626763 D1	24-04-2003
		DE 69626763 T2	05-02-2004
		EP 0779598 A2	18-06-1997
		JP 3492057 B2	03-02-2004
		JP H09167217 A	24-06-1997
		US 5838059 A	17-11-1998
