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

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
3 juin 2010 (03.06.2010)

PCT

(10) Numéro de publication internationale
WO 2010/061002 A1

(51) Classification internationale des brevets :
G06Q 20/00 (2006.01) *G06K 19/077* (2006.01)
G07F 7/08 (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2009/066034

(22) Date de dépôt international :
30 novembre 2009 (30.11.2009)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
08170309.2 28 novembre 2008 (28.11.2008) EP

(71) Déposant *(pour tous les États désignés sauf US)* : **GEMALTO SA** [FR/FR]; 6 rue de la Verrerie, F-92190 Meudon (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : **BOUCHER, Daniel** [CA/CA]; 886, Jules Poitras, Saint-Laurent, Quebec, H4N 3M7 (CA).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE,

[Suite sur la page suivante]

(54) Title : PORTABLE OBJECT INCLUDING A DISPLAY AND APPLICATION FOR CARRYING OUT ELECTRONIC TRANSACTIONS

(54) Titre : OBJET PORTABLE COMPORTANT UN AFFICHEUR ET APPLICATION À LA RÉALISATION DE TRANSACTIONS ÉLECTRONIQUES

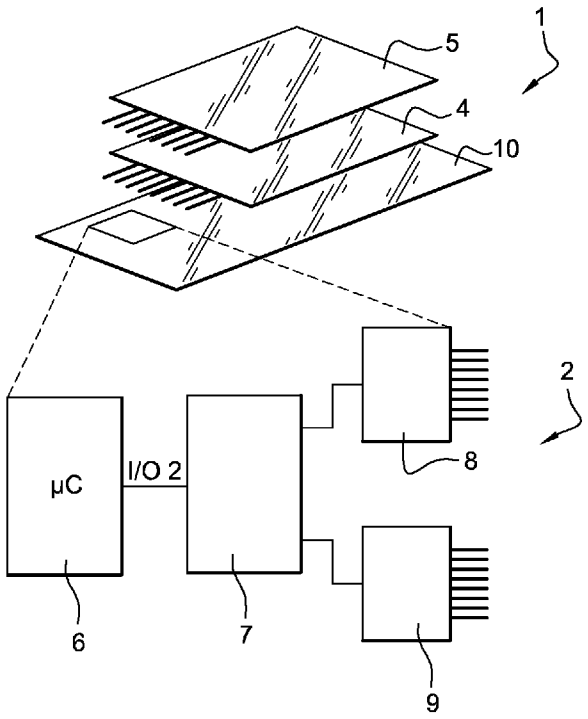

Fig. 1

(57) Abstract : The invention relates to a smart portable object comprising a safety component and a display, characterised in that the display is directly or indirectly interactive between a user and the safety component. The invention also relates to the use of a portable object for implementing an electronic transaction, including a display step for displaying all or some of the information that is useful to a user for the transaction and/or a step of interacting with the user, wherein the display and/or interaction step is carried out via said interactive display.

(57) Abrégé : L'invention concerne un objet portable intelligent comportant un composant de sécurité et un afficheur; Il se distingue en ce que l'afficheur est interactif directement ou indirectement entre un utilisateur et le composant de sécurité. L'invention concerne également une utilisation de l'objet portable pour mettre en œuvre une transaction électronique, comprenant une étape d'affichage pour présenter tout ou partie d'informations utiles à la transaction à un utilisateur et/ou une étape d'interaction avec l'utilisateur, l'étape d'affichage et/ou l'interaction étant réalisée(s) via ledit afficheur interactif.

WO 2010/061002 A1

ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

— *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii))*

Publiée :

— *avec rapport de recherche internationale (Art. 21(3))*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues (règle 48.2.h))*

Objet portable comportant un afficheur et application à la réalisation de transactions électroniques

L'invention concerne un objet portable comportant un afficheur, son utilisation pour mettre en œuvre des étapes d'un procédé de transaction électronique et le système associé.

En particulier, l'invention s'applique à la réalisation de transactions électroniques sécurisées telles que des paiements à l'aide d'un objet sécurisé portable tel qu'une carte à puce, clé USB, etc. Les paiements peuvent être en local à l'aide de terminaux de paiement ou en ligne sur internet en relation avec des sites et serveurs marchands ou unité de traitement associée distante ou locale. L'objet se présente sous la forme d'une carte à puce dans un mode de réalisation préféré.

Bien que décrit en relation avec un exemple de transaction financière, le terme transaction désigne ici tout échange bidirectionnel entre l'objet portable et une unité de traitement, par exemple une consultation de base de données, de base personnelle sécurisée, un accès à des fichiers partagés, un téléchargement, un contrôle d'accès, des traitements de données de type monétaire comme les transferts de fonds....

De tels objets portables sont connus parmi les cartes à puce pour afficher notamment des soldes de transactions, le contenu d'une mémoire, un numéro OTP (one time pass word en terminologie anglo-saxonne). De telles cartes peuvent être autonomes et avoir une batterie et un bouton pour actionner la génération de l'OTP. Certaines cartes contiennent un afficheur du type OLED pour présenter des informations alphanumériques.

On connait aussi des étiquettes électroniques pour supermarché ou étalage comportant un afficheur et ayant une interface capable de recevoir des

informations particulièrement de prix et de mise à jour par communication radiofréquence avec une unité centrale de chargement de données.

On connait aussi des appareils portables communicants tels que des dispositifs assistants personnels & téléphones (PDA Phone) comportant des afficheurs sensitifs tel que "iPhone" de la société Apple.

On connait aussi les terminaux bancaires lecteur de carte à puce et à bande magnétique capables d'effectuer une transaction électronique. De tels terminaux sont susceptibles de présenter des chevaux de Troie et ne présentent pas une garantie et sécurité suffisante pour un utilisateur.

Pour sécuriser les transactions, on a recours à des transactions en ligne conforme au standard EMV (ex:Mastercard EMV-CAP). Actuellement, il existe trois modèles d'authentification de domaine (3-D sécurisé par Visa, secureCode par Mastercard, ou J/secure par JCB International).

Toutefois, les transactions en ligne sont plus complexes que les transactions en magasins car il faut saisir plus de données.

L'invention a pour objectif de résoudre les inconvénients précités.

La présente invention propose dans son principe un objet portable dont la structure permet de rendre plus difficile de telles fraudes dans les transactions avec des terminaux de paiement ainsi qu'un nouveau schéma de transaction utilisant cet objet portable.

Selon l'invention, l'objet portable comporte un écran interactif apte à afficher une partie au moins des données utiles à la transaction. Ainsi, les données saisies par l'utilisateur peuvent être envoyées directement de l'objet portable de confiance à une unité de traitement de confiance, notamment à un organisme émetteur de l'objet ou l'accréditant. De même, les données émises

de l'unité de traitement de confiance peuvent être reçues directement par l'objet portable et présentées avec confiance sous le contrôle de l'objet.

A cet effet, l'invention concerne objet portable intelligent comportant un composant de sécurité et un afficheur interactif; il est caractérisé en ce qu'il est apte à réaliser des transactions interactives avec une unité distante telle qu'une banque, à travers l'afficheur interactif et sous le contrôle direct ou indirect d'un composant de sécurité.

Les données tapées par l'utilisateur sur l'écran sont reçues ou décodées par un contrôleur graphique sécurisé et/ou une puce comprenant un contrôleur sécurisé et/ou mettant en œuvre des opérations de sécurité.

Ainsi, l'afficheur interactif, par exemple sensitif au toucher, permet de réaliser la transaction directement entre la carte à puce et une unité de traitement, en rendant plus difficile des attaques frauduleuses et améliorant ainsi la sécurité. Le cas échéant, un protocole de communication sécurisé, notamment chiffré peut être partagé entre le processeur de l'objet et l'unité de traitement.

L'utilisateur peut ainsi dialoguer avec son objet portable en toute confiance directement. L'objet a l'avantage d'économiser un clavier ou autre interface homme machine et offre une surface utile d'affichage plus grande ou permet de rendre l'objet plus petit par exemple au format Mini UICC ou mini SIM tout en incorporant une interface homme machine IHM.

Dans le cas d'une carte, l'usage d'un lecteur de type transparent du demandeur, illustré sur les figures ou un lecteur radiofréquence ne couvrant pas la carte ou l'objet, permet de rendre visible et accessible la surface de l'objet ou se trouve l'écran interactif.

L'interactivité peut être obtenue par exemple par des capteurs de pression ou autre, capacitifs, résistifs, magnétiques placés derrière ou combinés à un écran souple.

Selon d'autres caractéristiques, l'objet portable comprend seul ou de manière combinée:

- une interface de communication avec un terminal, celle-ci pouvant être une interface de toute nature à contact ou radiofréquence, voire même par exemple de simples connecteurs électriques pour une connexion de type ohmique avec un port de terminal;

- des moyens de communication aptes à établir une communication avec une unité de traitement distante et/ou afficher des informations provenant de l'unité de traitement distante;

- L'objet portable est apte à faire transiter les données saisies sur l'écran à l'unité distante;

- Il est apte à interagir directement via l'écran avec un utilisateur;

- Il comprend un programme ou protocole permettant d'afficher des données d'une transaction en provenance de l'unité distante pour approbation et/ ou contrôle par interaction sur une zone affiché sur l'écran;

- Il comprend un programme ou protocole permettant d'afficher au moins un mode de paiement et de transmettre un mode sélectionné par interaction sur une zone affichée sur l'écran;

- Il comprend un programme permettant d'afficher au moins un clavier interactif de saisie d'un code PIN et de transmettre pour vérification le code PIN sélectionné par interaction avec les zones affichées sur l'écran;

- Il comprend un programme capable d'afficher au moins une zone d'écriture et de transmettre pour vérification des paramètres de saisie de l'écriture par interaction avec l'écran.

L'invention a également pour objet un procédé (et système correspondant) pour réaliser une transaction électronique comprenant un échange de données entre une unité de traitement distante et un objet portable, l'unité étant connectée à l'objet portable, ledit procédé mettant en œuvre :

- une étape d'affichage pour présenter tout ou partie d'informations utiles à la transaction à un utilisateur

- et/ou une étape d'interaction avec l'utilisateur, caractérisé en ce que l'objet portable utilisé est conforme à l'une des revendications précédentes et en ce que l'étape d'affichage et/ou l'interaction sont réalisée(s) via ledit afficheur interactif.

Le système comprend un lecteur de carte qui est agencée par rapport à la carte de manière à laisser l'afficheur interactif utilisable (accessible) et visible par l'utilisateur une fois placée en position de communication dans le lecteur.

Grâce à l'invention, les terminaux bancaires peuvent être remplacés par tout lecteur de carte classique car la transaction a lieu directement entre la carte à puce et l'organisme bancaire émetteur de la carte. A la limite le lecteur peut être un simple connecteur sans électronique ou sans effectuer une interface logicielle.

Elle permet également la convergence de tous les systèmes de paiement via internet que les achats / transactions soient effectués en magasin ou en ligne via internet une fois que le marchand a obtenu les données d'identification de son institution financière ou portail de paiement sécurisé. En outre, le procédé basé sur un modèle de transaction basé sur internet permet d'éviter des frais de communication téléphonique.

Grâce au lecteur de carte connecté à l'ordinateur, l'utilisateur peut maintenant avoir la même expérience de transaction en ligne que s'il effectuait une transaction locale en magasin sans avoir besoin d'entrer son numéro de carte ou autre information requise par les marchands en ligne actuels.

Un avantage important de l'invention est que l'identité de l'acheteur et le mode de paiement sont uniquement connus par l'acheteur et la banque émettrice; L'unique information connue du portail de paiement et le marchand sont la banque émettrice et confirmation du montant de la transaction.

Le client peut utiliser un ou plusieurs modes de paiement dans la même transaction dans le cas notamment ou un compte est insuffisamment approvisionné.

D'autres particularités et avantages de l'invention apparaîtront à la lecture de la description, faite à titre d'exemple non limitatif et en regard des dessins annexés sur lesquels :

- La figure 1 illustre schématiquement la structure d'un objet portable conforme à l'invention;

- La figure 2 illustre schématiquement une utilisation de l'objet conforme à l'invention à l'aide d'un connecteur/lecteur;

- La figure 3 illustre schématiquement le réseau du site marchand pour utiliser l'invention selon un mode de mise en œuvre;

A la figure 1, l'objet portable servant à la description d'exemple de réalisation est une carte à puce 1 notamment au format ISO 7816; mais il pourrait être tout objet portable intelligent à microcircuit tel une clé USB ou carte à d'autres formats PCMCIA, MMC. Le microcircuit présente de préférence des fonctions de sécurité propres aux cartes à puce (protections physiques et/ou logiques, par exemple : clé de chiffrement, moyens anti intrusion, authentification, élaboration de certificat, génération de données aléatoires, brouillage de données,...); il est logé ici dans un module à contacts électriques 2 mais pourrait avoir des fonctions ou interface de communication autres telle une fonction sans contact notamment radiofréquence RFID selon la norme ISO 14443. L'objet portable est en principe destiné à communiquer avec un terminal de communication directement ou par l'intermédiaire d'un connecteur et/ou lecteur associé. Le microcircuit peut être dans une carte connecté à un objet ou soudé à un circuit électronique de l'objet

Dans la mesure où la couche OLED ou papier électronique pourrait être translucide notamment lorsqu'il n'y a pas du courant, les couches 4 et/ou 5 ou 10 pourraient comprendre des éléments de sécurité tels que des logos, des graphiques et hologrammes imprimés sous ces couches de manière conventionnelle pour renforcer la sécurité de la carte ou objet. Ces éléments de sécurité peuvent être réalisés par autre moyens tels que laser de personnalisation. Ainsi, la carte peut comprendre sur une face ou visible par

transparence des couches tous les éléments nécessaires classiques de sécurisation graphique.

Dans une variante de réalisation, l'objet peut fonctionner en mode indépendant sur lui même sans communiquer avec le terminal; Notamment, il peut être amené à effectuer des fonctions de consultations d'une mémoire interne, ou génération de numéro OTP ou autres fonctions de saisie, sauvegarde ou comme une calculatrice.

Dans le cas d'une clé USB, la clé peut être enfichée dans un port de terminal de communication, PC, PDA, téléphone portable, etc. Dans l'exemple, la carte est reliée au terminal à l'aide d'un lecteur de carte ISO.

Le format carte à puce est préféré notamment pour des raisons de sécurité et portabilité de la carte et autres utilisations possibles parallèles: carte prépayée, fidélité, etc.

L'objet comporte ou est connecté à un afficheur 4 (écran) de préférence graphique mais pourrait simplement être de type alphanumérique.

Selon une caractéristique de l'invention, l'afficheur est interactif. L'interactivité de l'écran peut être obtenue par exemple par des capteurs de pression ou autre, capacitifs, résistifs, magnétiques placés derrière ou combinés à un écran, de préférence souple.

Dans l'exemple, on utilise de préférence un afficheur sensitif au toucher d'un doigt ou autre ustensile associé, pointe, stylo.

L'afficheur comprend dans l'exemple une couche d'afficheur 4 de type papier électronique (OLED) combinée à une couche sensible ou tactile 5.

L'afficheur s'étend de préférence sur une surface de l'ordre du 1/3 ou 1/2 de la surface de la carte sur une portion de surface et comporte une zone

distante du module pour permettre une visibilité de la carte quand elle est insérée dans le connecteur.

De manière avantageuse le connecteur C/L associé à la carte est agencé structurellement de manière à permettre une interaction de l'utilisateur avec l'afficheur interactif. Ici, le lecteur comporte des bras 11, 12 échancrés en "V" (figure 2). L'afficheur n'est donc pas couvert par le boitier du connecteur. Le lecteur est aussi agencé par rapport à la carte de manière à laisser l'afficheur interactif de la carte accessible et visible par l'utilisateur une fois placé en position de communication dans le lecteur.

Toutefois, l'afficheur pourrait couvrir la quasi totalité ou totalité de cette surface. Un connecteur éventuel à contacts électriques peut être localisé de préférence du même côté que l'afficheur mais pourrait être placé sur la face opposée pour gagner en surface.

L'objet est apte à interagir directement via l'écran avec un utilisateur.

Les deux couches sont reliées respectivement de manière connue à des moyens ou microcircuits électroniques 2 aptes à assurer les fonctions de présentation d'information à un utilisateur et à recevoir de manière interactive des interactions de l'utilisateur notamment par pression sur la couche tactile 5 .

Les moyens électroniques comprennent dans l'exemple un premier microcontrôleur 6 de carte à puce standard relié à au moins un second microcontrôleur 7 de l'écran sensitif et /ou de l'écran graphique par une connexion I/02 sur le second port série du microcontrôleur de la carte à puce, le premier port étant utilisé pour la communication via les contacts notamment ISO 7812-2). Le second microcontrôleur 7 pilote respectivement les deux couches par un décodeur d'adresse ou interface 8, 9.

Physiquement, on peut avoir une puce par microcontrôleur, connectées ensemble l'une sur l'autre et logées ensemble dans un module de carte à puce. Le cas échéant, l'ensemble des fonctions décrites ci-dessus peuvent être intégrés dans un seul composant ou réparties dans plusieurs composants positionnés et noyés dans le corps en plastique 10 de la carte à puce selon une technologie de carte à puce multi composants dans laquelle, les composants sont reliés par des pistes électriques réalisées sur un support souple notamment par gravure ou sérigraphie ou jet d'encre, etc.

De préférence, l'interaction avec l'utilisateur s'effectue directement ou indirectement entre l'écran et un composant de sécurité. Dans l'exemple, les données vont au composant de sécurité 6 via le contrôleur graphique et/ou tactile 7 qui peut aussi être sécurisé.

Les données vont directement dans un composant de sécurité ou passent le cas échéant par un composant de préférence également sécurisé. Il peut exister une procédure d'authentification mutuelle ou réciproque entre les deux composants, pour éviter par exemple une substitution de puce.

Dans une variante de mise en œuvre, la carte peut être une carte de type PCMCIA ou autre et comprendre une mémoire partagée accessible directement par une unité de traitement hôte et par un microcontrôleur de la carte. Les données à échanger avec l'hôte puis une unité distante, transitent par cette mémoire. Un fonctionnement comme celui du dispositif de communication entrée /sortie décrit dans le brevet EP0649547 peut être retenu pour mettre en œuvre l'invention, l'afficheur et l'écran pouvant être considérés comme interface d'entrée /sortie.

Les sélections sur l'écran sont perçues et décodées ou interprétées par le micro contrôleur 7. Par exemple, un code PIN tapé éventuellement selon une logique connue de l'utilisateur et partagée par le microcontrôleur 7 est déduit par le microcontrôleur. Le microcontrôleur 7 transpose éventuellement les signaux perçus en données représentant le code PIN.

Ces données sont ensuite comparées soit dans le même composant sécurisé ou transmis à un autre composant sécurisé 6 pour comparaison ou transmission à un dispositif externe (serveur bancaire) pour comparaison avec un code PIN pré enregistré.

Les données représentant le code PIN sont communiquées au composant 7, le cas échéant, en mettant en œuvre un mécanisme de sécurité (chiffrement, ...)

Pour son fonctionnement l'objet portable comprend des fonctions et/ou moyens décrits ci-dessous de manière cumulative ou isolée.

Selon une autre caractéristique, l'objet portable comprend des moyens de communication aptes à établir une communication avec une unité de traitement distante et/ou afficher des informations provenant de l'unité de traitement distante. La carte comprend notamment des moyens permettant d'établir une communication sur internet directement ou indirectement via le terminal. Dans l'exemple, le protocole IP internet y est intégré et on dispose d'une communication directe sur internet par l'intermédiaire du terminal, ce dernier devenant transparent et intervenant comme un modem en réalisant juste l'interface de communication physique entre le réseau et la carte

Selon une caractéristique, la carte est apte à faire transiter les données saisies sur l'écran à l'unité distante; En particulier, les données saisies sont interprétées et/ou décodées par le contrôleur second avec son décodeur et transmises au contrôleur premier pour être véhiculées sur internet à une unité distante qui peut être un serveur d'un site marchand. Un programme d'interprétation P2 et un programme de transfert P3 des données saisies sont présents dans le second microcontrôleur 7 ou répartis entre les deux 7, 8.

Selon d'autres caractéristiques, la carte comprend un programme ou protocole P4 permettant d'afficher des données d'une transaction en provenance de l'unité distante pour approbation et/ ou contrôle par interaction sur une zone affiché sur l'écran.

Selon d'autres caractéristiques, la carte comprend un programme ou protocole P5 permettant d'afficher au moins un mode de paiement et de transmettre un mode sélectionné par interaction sur une zone affichée sur l'écran.

Elle comprend un programme PIN P6 permettant d'afficher au moins un clavier interactif de saisie d'un code PIN et de transmettre pour vérification le code PIN sélectionné par interaction avec les zones affichées sur l'écran.

La vérification peut s'effectuer de préférence par un serveur distant officiel (banque, ...) mais peut s'effectuer dans la carte de manière plus classique; Dans ce dernier cas, le terminal reçoit la réponse de la carte ou un certificat permettant de réaliser la transaction. De préférence, la carte valide le PIN elle-même pour une pré-validation avant de transmettre à la banque. Il est à noter qu'un logiciel de traitement de changement de PIN avec synchronisation avec la banque est également envisageable en option.

La carte comprend un programme P7 de saisie biométrique telle une écriture, une signature. La signature peut être réalisée sur l'écran tactile avec un stylet; En particulier, le programme est apte à faire afficher au moins une zone d'écriture sur l'écran et de transmettre pour vérification des paramètres de saisie de l'écriture par interaction avec l'écran. La carte peut également à cet effet comprendre des moyens d'analyse et diagnostic des données saisies, par exemple une comparaison ou calcul de la dynamique de la signature. Le cas échéant, un capteur biométrique et/ou d'empreinte peut être associé à la surface de la carte ou à côté de l'écran tactile; ces données peuvent venir compléter une saisie de PIN code ou constituer les données à vérifier pour la

transaction. La carte peut comprendre un programme de reconnaissance statique d'une signature et/ou écriture dynamique d'une signature sur un écran sensitif.

Une utilisation de l'objet conforme à l'invention est décrite maintenant en relation avec la figure 2 qui illustre le procédé et/ou système pour réaliser une transaction électronique comprenant un échange de données entre une unité de traitement distante connectée à un objet portable.

Le procédé met en œuvre une étape d'affichage pour présenter tout ou partie d'informations utiles à la transaction à un utilisateur et/ou une étape d'interaction et/ou validation de l'utilisateur. Bien que préférable d'effectuer ces opérations à l'aide de l'afficheur interactif de l'invention, l'invention permet d'utiliser cet afficheur interactif pour réaliser tout ou partie d'au moins l'étape d'affichage ou d'au moins celle de l'interaction sécurisée. Ainsi par exemple, la confirmation du montant et/ou la sélection du mode pourrait être toujours effectuée sur un autre clavier que celui de la carte. Les différentes étapes et interactions pourraient être réparties entre la carte et le système (écran PC, clavier PC ou clavier du et afficheur du terminal POS).

Pour réaliser une transaction sur internet, l'utilisateur se connecte à un réseau de communication tel internet avec son ordinateur PC et sélectionne sur un site marchand un produit ou service à acheter. Le PC comprend une interface carte à puce réalisée ici par un connecteur ou lecteur C/L. Le connecteur peut être relié aussi par un câble USB au PC et la communication et fonction USB peuvent être réalisées soit par la carte elle-même, soit par une fonction d'adaptation ISO/USB du lecteur.

Au cours de la transaction ou avant, l'utilisateur introduit sa carte dans un connecteur adapté relié au terminal et les données et opérations nécessaires à la transaction sont alors réalisées entre la carte et le réseau. L'utilisateur peut être invité à introduire sa carte par un message émis ou

véhiculé du site marchand et affiché à l'écran du PC comme si il était notamment à une caisse de supermarché.

L'utilisateur introduit sa carte qui est alors détectée par le PC et la communication peut être basculée directement entre la carte et le réseau via les connexions du terminal. Dans le cas contraire, la communication peut s'effectuer via le PC comme interface logique et physique qui relaye les communications à la carte.

Le portail de paiement a fait préalablement une requête à la banque du client qui établit ensuite une communication avec la carte pour effectuer une transaction sécurisée comme si la carte était dans un lecteur de paiement portable POS.

On parvient alors dans le cadre d'une communication sécurisée C5 dont l'établissement est décrit ultérieurement, entre la carte et la banque émettrice du client.

Ensuite, le paiement en lui même est effectué de la manière suivante :

- A l'étape 100 le site marchand ayant communiqué à la banque (notamment à travers une requête de paiement à un portail de paiement 16 expliqué ci-dessous) les données de la transaction à la carte, par exemple un montant de $ 12.50, la banque fait afficher le montant de la transaction par une commande d'affichage destinée à la carte et comportant le montant à afficher comme donnée liée à la commande.

Les questions "continuer" et deux réponses "oui", "non" à l'intérieur ou en regard de deux fenêtres distinctes interactives de l'afficheur sensitif sont également affichées soit à l'initiative de la banque par une commande équivalente à la précédente soit à l'initiative de la carte qui comprend un programme apte à afficher ces questions déclenchées par la réception de la commande précédente.

A l'étape 200, l'utilisateur ayant sélectionné "oui", un signal correspondant est capté par le contrôleur de la carte et retourné à la banque;

La banque fait ensuite afficher ou véhiculer à destination de la carte, un menu de sélection du mode de paiement comprenant par exemple : par carte porte monnaie électronique, carte de débit, carte de crédit, ou carte de crédit de points de fidélité. Ces options sont affichées dans des zones interactives respectivement E1, E2, E3, E4 de la couche interactive en regard de l'afficheur.

Alternativement, l'initiative peut provenir de la carte qui comprend au préalable une liste des possibilités de paiement offerte à l'utilisateur et qui déclenche elle-même grâce à un programme applicatif approprié exécuté par le microcontrôleur de la carte en réponse à la sélection de la réponse "oui".

Une fois sélectionnée, la zone points de fidélité est détectée par le site marchand qui renvoie un clavier de saisie de PIN code avec des touches interactives. Le clavier est de préférence brouillé ou chiffré et déchiffré dans la carte.

Alternativement, l'initiative de l'affichage d'un code PIN peut provenir de la carte en vertu d'un programme qui fait afficher un code PIN, éventuellement modifié à chaque affichage selon une séquence connue de l'utilisateur. L'affichage est déclenché en réponse à la sélection précédente du mode de paiement capté par la carte.

Des étoiles s'affichent sur l'écran à chaque saisie de numéro et une validation sur "OK" déclenche l'envoi du code PIN sur le réseau à destination de la banque, ceci étant effectué de préférence sous forme chiffrée grâce à des clés de chiffrement préalablement chargées ou générées et algorithmes de chiffrement et/ou vérification de certificat de la carte.

Alternativement, la carte reçoit elle-même le code PIN et le vérifie elle-même, puis communique un résultat positif de la vérification de préférence sous forme chiffrée à la banque ou avec un certificat associé.

A l'étape 400, la banque du client a vérifié le PIN reçu qu'elle a, le cas échéant, déchiffré au préalable et fait afficher une information indiquant le

succès de la transaction à destination de la carte également sous forme de commande d'affichage et la banque procède ensuite au paiement.

Alternativement, la carte a vérifié le code PIN en interne et communique sous forme chiffrée de préférence le résultat positif de la comparaison du code PIN tapé à la banque qui déchiffre en local et procède au paiement.

Ensuite, des messages de confirmation de paiement interviennent entre la banque et le portail de paiement (voir liaison C6, C7) qui en informe le serveur marchand et un transfert de fond et finalisation de la transaction intervient de la banque du client à celle du marchand.

La figure 3 illustre schématiquement le réseau du site marchand pour utiliser l'invention selon un mode de mise en œuvre.

Par simplification, le portail de paiement intervient aussi comme autorité de certification;

Pour les transactions en ligne, le terminal de paiement peut être un PC connecté via une connexion internet;

Dans le cas de remboursement, le serveur de la banque émettrice et le serveur de la banque débitrice sont permutés;

Le système de l'invention comprend le terminal PC relié à la carte pour se connecter à une unité de traitement distante 15, 16 telle un serveur marchand 15 via un réseau quelconque tel Wifi, Ethernet, internet 15, 17 et/ou une banque émettrice de l'utilisateur 17. Ces unités 15, 17 sont aptes à mettre en œuvre un protocole de communication et/ou jeu de commandes avec l'objet portable permettant l'affichage et/ou une récupération des données saisies à l'écran directement et/ou après traitement et/ou vérification par l'objet portable.

Le serveur marchand 15 est en relation de communication avec une banque réceptrice 18 d'une part et un portail de paiement 16 d'autre part. Le

portail de paiement 16 est en relation avec la banque du client 17 et celle 18 du marchand.

Les étapes sont les suivantes :

C1 : Une communication sécurisée C1 telle que du type TSL/SSL est établie entre le serveur marchand 15 et le portail de paiement 16;

C2: Le montant de la transaction, l'identité du serveur, l'identité de la banque émettrice et identité du serveur de la banque réceptrice sont chiffrés et transmis C2 au portail de paiement 16 en utilisant la clé publique du portail de paiement.

C3: Une communication sécurisée C3 telle que du type TSL/SSL est établie entre le portail de paiement 16 et le serveur marchand de la banque émettrice 17;

C4 : Une communication sécurisée C4 telle que du type TSL/SSL est également établie entre serveur marchand 15 et le serveur de la banque réceptrice 18;

C5 : Une liaison sécurisée C5 est établie entre la banque émettrice et la carte (voir plus loin pour détail), confirmation de retrait retourné au portail de paiement via le portail de paiement et serveur marchand ou directement via le PC.

C6 : Une liaison sécurisée C6 est établie entre la banque réceptrice et la carte du marchand, confirmation de dépôt retournée au portail de paiement 16.

C7- Un numéro de confirmation de transaction est retourné au marchand (et par conséquent aussi à la carte du client).

Les éléments ci-après doivent de préférence être injectés selon un exemple de mise en œuvre, dans la carte client au cours d'une personnalisation (ou lors de l'émission de la carte) pour sécuriser la transaction notamment entre la banque émettrice et la carte du client.

IDcc = identifiant de la carte client

CERTca = CA certificat

CERTcc = Certificat de la carte client (Date d'expiration) avec Pukcc = clé publique de la carte client

PrKcc = parties de clé privée de la carte client (P, Q, PQ, Exposant DP et exposant DQ)

Skcc = Clé secrète de la carte client partagée avec la banque émettrice.

La banque (ou serveur équivalent) de son côté comprend également des moyens pour chiffrer les données émises vers la carte et déchiffrer les données reçues de la carte.

La banque (ou serveur équivalent) comprend également des moyens pour élaborer un certificat à destination de la carte ou vérifier un certificat reçu de la carte.

Selon d'autres caractéristiques alternatives ou complémentaires, une fois la liaison sécurisée établie entre la carte et la banque émettrice de la carte, celle-ci peut proposer via l'interface affichable de la carte, les différents types de paiement disponibles.

La carte peut communiquer directement avec la banque de manière interactive. Pour cela, un jeu de commande et/ou protocole sont partagé(s) entre la carte et la banque. Des messages de la banque à la carte sont transmis directement et inversement, le cas échéant encapsulés dans un protocole de communication du réseau.

La carte comprend le cas échéant un autre protocole et jeu de commandes propres à la banque émettrice qui est déclenchée une fois la communication établie entre la carte et la banque. Le lecteur est apte à encapsuler/des encapsuler les commandes et données provenant de la carte et inversement.

Les menus et les types de transactions sont véhiculés de manière interactive de la banque vers la carte. En d'autres mots, les types de paiement disponibles en concordance avec le profil du client (ex : compte bancaire 1, compte bancaire 2, compte de crédit 1, marge de crédit...) sont offerts ou proposés directement par la banque avec les montants (balance) disponibles sur ces comptes (ex : compte bancaire 1 à 2000 €, compte bancaire 2 à 1500 €,

balance du compte de crédit 1 à 500 €...); L'invention permet d'effectuer un paiement réparti sur plusieurs comptes selon le crédit disponible sur chaque compte ou au choix du client.

5

REVENDICATIONS

1. Objet portable intelligent (1) comportant un composant de sécurité (6) et un afficheur (5) interactif, caractérisé en ce qu'il est apte à réaliser des transactions interactives avec une unité distante telle qu'une banque, à travers l'afficheur interactif et sous le contrôle direct ou indirect d'un composant de sécurité (6, 7).

2. Objet portable selon la revendication précédente, caractérisé en ce qu'il est comprend ou constitue une carte à puce.

3. Objet portable selon la revendication précédente, caractérisé en ce que la carte est apte à mettre en œuvre un protocole de communication et/ou jeu de commandes partagé(s) avec une l'unité distante pour communiquer directement avec elle.

4. Objet portable selon l'une des revendications 1 à 3, caractérisé en ce qu'il comprend une interface de communication avec un terminal (PC).

5. Objet portable selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend des moyens de communication physiques et/ou programmes (P2, P3) aptes à établir une communication avec une unité de traitement distante (15, 16, 17) et/ou afficher des informations provenant de l'unité de traitement distante.

6. Objet portable selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il est apte à faire transiter les données saisies sur l'écran (5) à l'unité distante.

7. Objet portable selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend un programme ou protocole (P4) permettant d'afficher des données d'une transaction en provenance de l'unité distante pour

approbation et/ ou contrôle de l'utilisateur par interaction sur une zone affichée sur l'écran.

8. Objet portable selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend un programme ou protocole (P5) permettant d'afficher au moins un mode de paiement et de transmettre un mode sélectionné par interaction de l'utilisateur sur une zone affichée sur l'écran.

9. Objet portable selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend un programme (P6) permettant d'afficher au moins un clavier interactif de saisie d'un code PIN et de transmettre pour vérification le code PIN sélectionné par interaction de l'utilisateur avec les zones affichées sur l'écran.

10. Objet portable selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend un programme de saisie biométrique ou reconnaissance de caractère statique et/ou dynamique (P7) capable d'afficher au moins une zone d'écriture et de transmettre pour vérification des paramètres de saisie de l'écriture par interaction de l'utilisateur avec l'écran.

11. Procédé pour réaliser une transaction électronique comprenant un échange de données antre une unité de traitement distante (15, 16, 17) et un objet portable (1), ledit procédé mettant en œuvre :

- une étape d'affichage pour présenter tout ou partie d'informations utiles à la transaction à un utilisateur,
- et/ou une étape d'interaction avec l'utilisateur,

caractérisé en ce que l'objet portable utilisé est conforme à l'une des revendications précédentes et en ce que l'étape d'affichage et/ou l'interaction sont réalisée(s) via ledit afficheur interactif (5).

12. Système pour réaliser une transaction électronique comprenant un échange de données bidirectionnel entre une unité de traitement distante et un objet portable, ledit système comportant :

- des moyens d'affichage pour présenter tout ou partie d'informations utiles à la transaction à un utilisateur
- et/ou des moyens d'interaction avec l'utilisateur,

caractérisé en ce que l'objet portable utilisé est conforme à l'une des revendications 1 à 10 et en ce que l'étape d'affichage et/ou l'interaction sont réalisée(s) via ledit afficheur interactif.

13. Système selon la revendication précédente, caractérisé en ce qu'il comprend une unité de traitement distante apte à mettre en œuvre un protocole de communication et/ou jeu de commandes avec l'objet portable permettant l'affichage et/ou une récupération des données saisies à l'écran directement ou après traitement ou vérification par l'objet portable.

14. Système selon l'une des revendications 12 ou 13, caractérisé en ce qu'il comprend un lecteur de carte qui est agencée par rapport à la carte de manière à laisser l'afficheur interactif accessible et visible par l'utilisateur une fois placée en position de communication dans le lecteur.

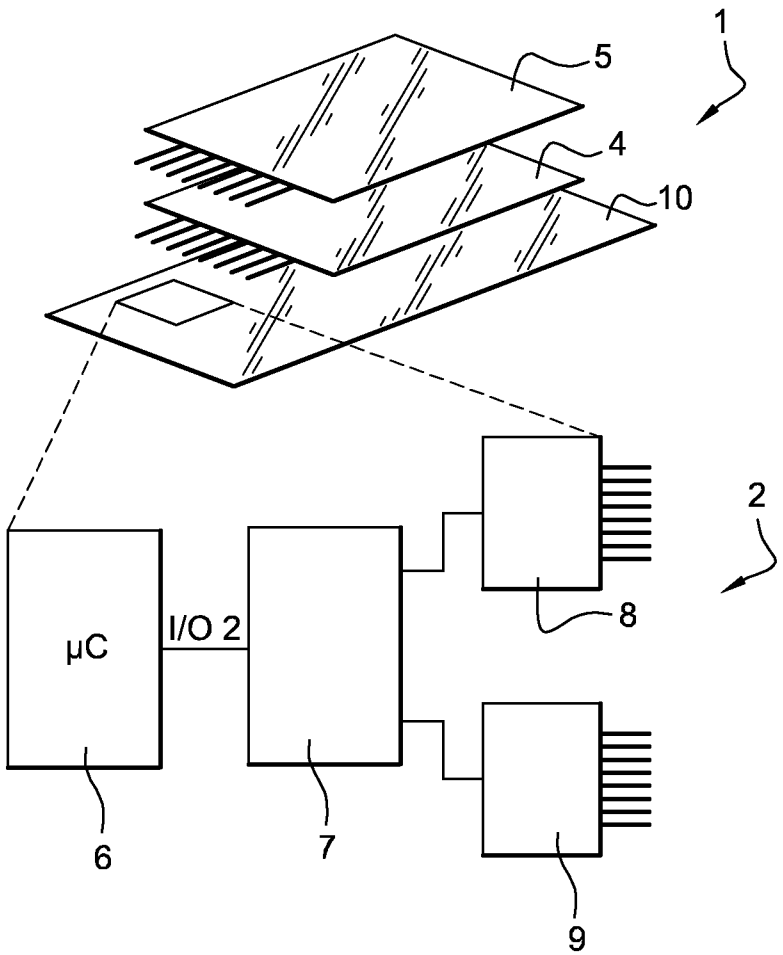

Fig. 1

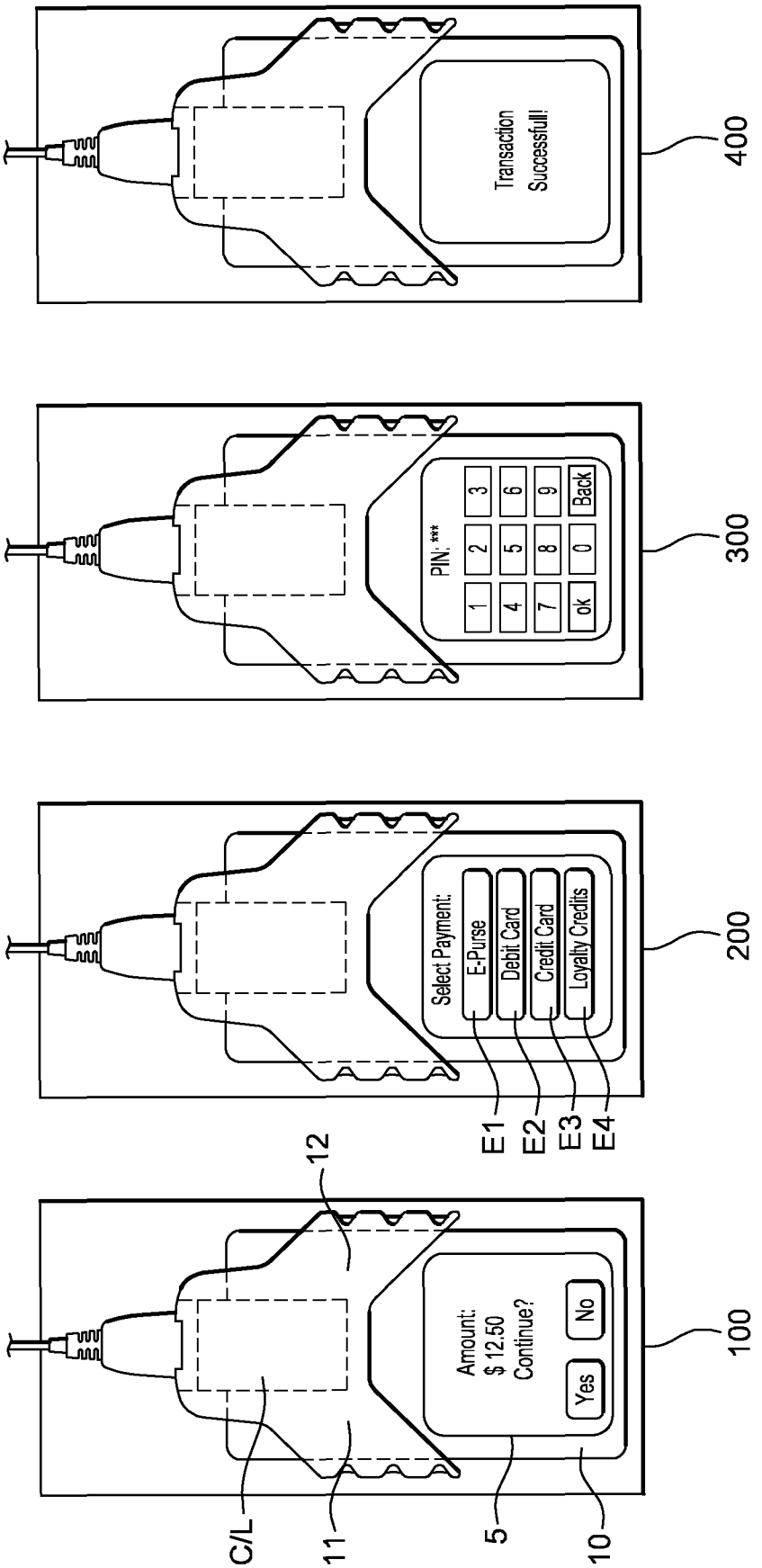
Amount:
$ 12.50
Continue?
Yes
No
100
C/L
11
12
5
10
Select Payment:
E-Purse
Debit Card
Credit Card
Loyalty Credits
200
E1
E2
E3
E4
PIN: ***
1
2
3
4
5
6
7
8
9
ok
0
Back
300
Transaction
Successfull!
400

Fig. 2

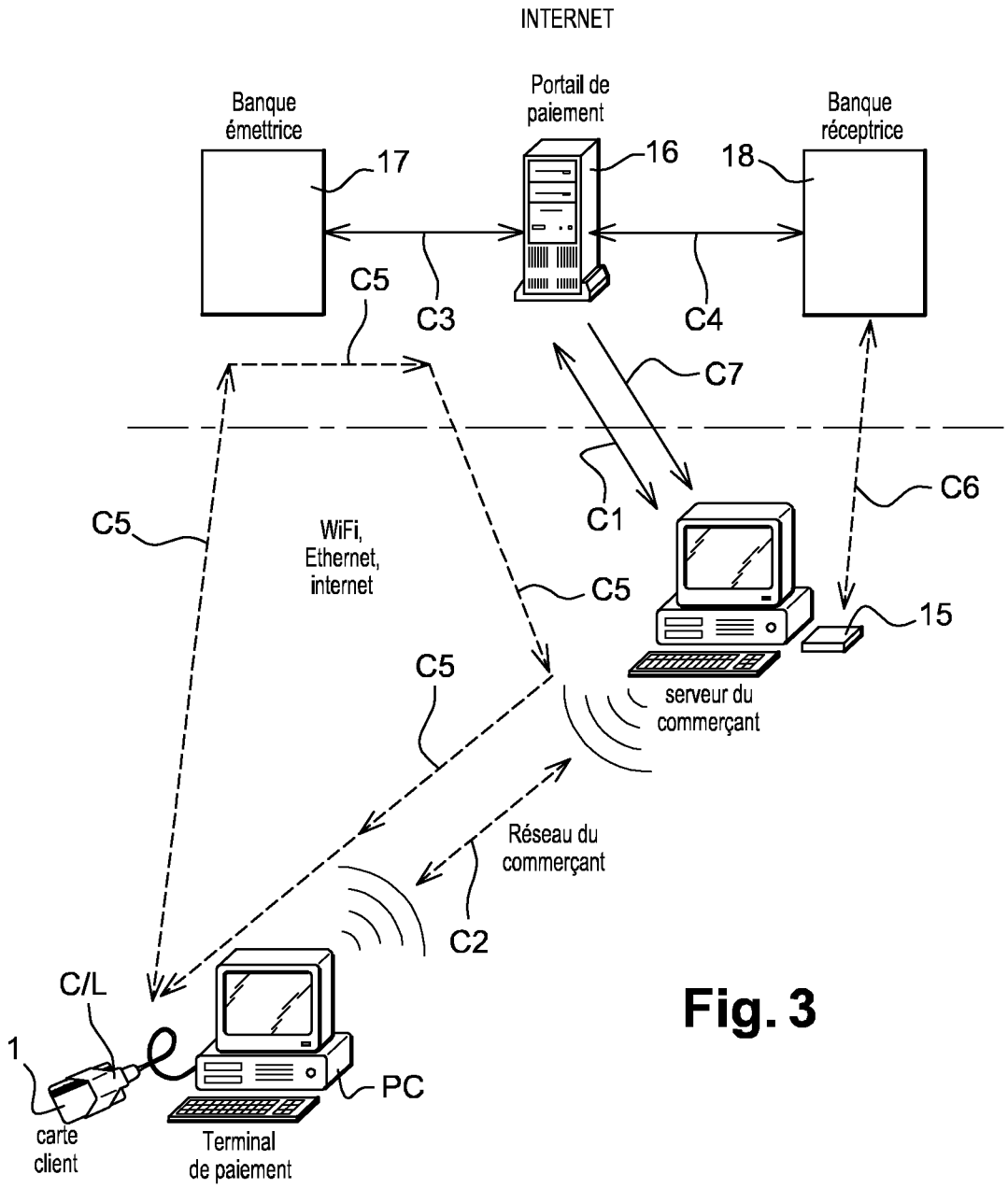
INTERNET
Banque émettrice
Portail de paiement
Banque réceptrice
17
16
18
C5
C3
C4
C7
C1
C6
C5
WiFi, Ethernet, internet
C5
15
C5
serveur du commerçant
Réseau du commerçant
C2
C/L
1
PC
carte client
Terminal de paiement

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2009/066034

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q20/00 G07F7/08 G06K19/077

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)
G06K G07F G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 980 053 A (CITIBANK NA [US]) 16 February 2000 (2000-02-16) paragraphs [0038], [0042], [0049], [0051], [0058], [0059], [0099]; claims 1-30; figures 1,2,5a,5b,7,17	1-14
X	US 2007/027804 A1 (VEGA EDWIN [US]) 1 February 2007 (2007-02-01) claim 1; figures 1-4	1-14
A	US 2006/131393 A1 (COK RONALD S [US] ET AL) 22 June 2006 (2006-06-22) paragraph [0038]; claims 1-4	1-14
A	EP 0 649 547 B1 (GEMPLUS CARD INT [FR]) 11 June 1997 (1997-06-11) cited in the application the whole document	1-14

☐ Further documents are listed in the continuation of Box C.

☒ See patent family 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
12 March 2010	31/03/2010

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, Fax: (+31-70) 340-3016	Closa, Daniel

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2009/066034

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0980053 A	16-02-2000	AU 732373 B2	26-04-2001
		AU 4353099 A	16-03-2000
		JP 2000200319 A	18-07-2000
US 2007027804 A1	01-02-2007	NONE	
US 2006131393 A1	22-06-2006	NONE	
EP 0649547 B1	11-06-1997	DE 69311554 D1	17-07-1997
		DE 69311554 T2	08-01-1998
		EP 0649547 A1	26-04-1995
		ES 2102660 T3	01-08-1997
		FR 2693575 A1	14-01-1994
		WO 9401822 A1	20-01-1994
		JP 3743677 B2	08-02-2006
		JP 7508843 T	28-09-1995
		JP 2005044375 A	17-02-2005
		SG 52634 A1	28-09-1998
		US 5802325 A	01-09-1998

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2009/066034

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06Q20/00 G07F7/08 G06K19/077

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)
G06K G07F G06Q

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	EP 0 980 053 A (CITIBANK NA [US]) 16 février 2000 (2000-02-16) alinéas [0038], [0042], [0049], [0051], [0058], [0059], [0099]; revendications 1-30; figures 1,2,5a,5b,7,17	1-14
X	US 2007/027804 A1 (VEGA EDWIN [US]) 1 février 2007 (2007-02-01) revendication 1; figures 1-4	1-14
A	US 2006/131393 A1 (COK RONALD S [US] ET AL) 22 juin 2006 (2006-06-22) alinéa [0038]; revendications 1-4	1-14
A	EP 0 649 547 B1 (GEMPLUS CARD INT [FR]) 11 juin 1997 (1997-06-11) cité dans la demande le document en entier	1-14

☐ 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'appartenant 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
12 mars 2010	31/03/2010

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, Fax: (+31-70) 340-3016	Closa, Daniel

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/EP2009/066034

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0980053 A	16-02-2000	AU 732373 B2	26-04-2001
		AU 4353099 A	16-03-2000
		JP 2000200319 A	18-07-2000
US 2007027804 A1	01-02-2007	AUCUN	
US 2006131393 A1	22-06-2006	AUCUN	
EP 0649547 B1	11-06-1997	DE 69311554 D1	17-07-1997
		DE 69311554 T2	08-01-1998
		EP 0649547 A1	26-04-1995
		ES 2102660 T3	01-08-1997
		FR 2693575 A1	14-01-1994
		WO 9401822 A1	20-01-1994
		JP 3743677 B2	08-02-2006
		JP 7508843 T	28-09-1995
		JP 2005044375 A	17-02-2005
		SG 52634 A1	28-09-1998
		US 5802325 A	01-09-1998