(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 892 875**

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **05 11081**

(51) Int Cl[8] : **H 04 L 9/14** (2006.01), G 06 F 7/58

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 28.10.05.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 04.05.07 Bulletin 07/18.

(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 :**

(71) **Demandeur(s) :** *GEMPLUS Société anonyme* — FR.

(72) **Inventeur(s) :** GIRARD PIERRE et VILLEGAS KARINE.

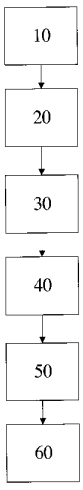
(73) **Titulaire(s) :**

(74) **Mandataire(s) :** BREESE DERAMBURE MAJEROWICZ.

(54) PROCEDE DE SECURISATION DES PAIEMENTS PAR DECOUPAGE DES MONTANTS.

(57) L'invention a pour objet un procédé pour réaliser une transaction d'un montant transactionnel (A) entre un moyen de paiement (1) et une institution de paiement (5) par l'intermédiaire d'un terminal de lecture (2), ledit moyen de paiement (1) comprenant au moins un processeur et une mémoire stockant une première information secrète (K) partagée avec ladite institution de paiement (5), ledit terminal de lecture (2) étant apte à transmettre des données audit moyen de paiement, le procédé étant caractérisé en ce qu'il comprend les étapes:

- de transmission (10) par ledit terminal de lecture (2), audit moyen de paiement (1), d'au moins ledit montant transactionnel (A);
- de génération (20) par ledit moyen de paiement (1), à l'aide dudit processeur, d'au moins une valeur de codage transactionnelle, ladite valeur de codage transactionnelle étant au moins fonction dudit montant transactionnel (A) et de ladite première information secrète (K);
- de transmission (40) dudit codage transactionnel à ladite institution de paiement;
- d'authentification (50, 60) par ladite institution de paiement, de ladite transaction correspondant audit montant transactionnel en fonction dudit codage transactionnel et de ladite première information secrète (K).



FR 2 892 875 - A1

PROCÉDÉ DE SÉCURISATION DES PAIEMENTS PAR DÉCOUPAGE DES MONTANTS

La présente invention concerne les procédés de sécurisation des transactions, par exemple dans le cadre d'un paiement par carte bancaire.

Dans ce cadre, la carte elle-même n'est souvent pas utilisée et l'information imprimée dessus est suffisante pour effectuer des achats par Internet, par téléphone, ou par fax.

Par exemple, le numéro de carte et la date d'expiration suffisent pour réaliser un achat sur Internet. Parfois, un cryptogramme imprimé au dos de la carte, et composé de trois chiffres en général, est également demandé pour l'authentification du possesseur de la carte. Cependant, le degré de sécurité rajouté par cette identification supplémentaire est faible puisque ce cryptogramme est facile à retrouver par une tierce personne.

La perte de la carte ou l'inattention de son possesseur qui laisserait un tiers voir ces données, entraînent donc un risque évident.

Un des buts de la présente invention est donc d'améliorer le niveau de sécurisation d'une transaction à partir d'un moyen de paiement tout en utilisant les infrastructures existantes telles que les téléphones, les ordinateurs, ou les fax.

Un autre but de la présente invention est d'empêcher un tiers mal intentionné de pouvoir faire facilement des achats à partir uniquement des données publiques d'un moyen de paiement, par exemple le numéro d'une carte bancaire et/ou sa date d'expiration.

Il est par ailleurs connu de pouvoir insérer dans une mémoire non volatile d'une carte bancaire, une information secrète uniquement partagée par la carte et l'institution bancaire. Pour cela, on stocke dans la mémoire de la carte au moment de sa fabrication, une clé secrète, qui est associée au numéro de série de la carte. La banque peut alors retrouver la relation entre le numéro de série et la clé par exemple à partir d'une base de données mettant en relation les numéros de série des cartes et les clés secrètes. De façon plus générale, la banque possède les moyens de retrouver la clé secrète d'une carte.

Cependant, cette clé secrète n'est pas utilisée dans des infrastructures de paiement telles que le téléphone, Internet, ou le fax.

Un autre but de la présente invention est de pouvoir utiliser une telle clé pour des paiements sur des infrastructures qui ne la prennent pas a priori comme paramètre.

On connaît également des lecteurs de cartes à puce pouvant être connectés par exemple sur des ordinateurs. Ces lecteurs sont aptes à alimenter la puce de la carte, à afficher des informations sur un écran et à recevoir des données par l'intermédiaire d'un clavier. Un tel lecteur de carte est par exemple commercialisé par la demanderesse sous le nom commercial GemPocket.

Un autre but de la présente invention est d'utiliser de tels lecteurs existants afin d'améliorer la sécurisation des transactions.

À cet effet, la présente invention a tout d'abord pour objet un procédé pour réaliser une transaction d'un montant transactionnel entre un moyen de paiement et une institution de paiement par l'intermédiaire d'un terminal de lecture, ledit moyen de paiement

comprenant un processeur et au moins une mémoire stockant une première information secrète partagée avec ladite institution de paiement, ledit terminal de lecture étant apte à transmettre des données audit moyen de paiement, ce procédé comprenant les étapes :

- de transmission par ledit terminal de lecture, audit moyen de paiement, d'au moins ledit montant transactionnel ;
- de génération par ledit moyen de paiement, à l'aide dudit processeur, d'au moins une valeur de codage transactionnelle, ladite valeur de codage transactionnelle étant au moins fonction dudit montant transactionnel et de ladite première information secrète ;
- de transmission de ladite valeur de codage transactionnelle à ladite institution de paiement ;
- d'authentification par ladite institution de paiement, de ladite transaction correspondant audit montant transactionnel en fonction de ladite valeur de codage transactionnelle et de ladite première information secrète.

Selon l'invention, on code donc un montant de transaction en au moins une valeur de codage transactionnelle, par exemple sous la forme d'une pluralité de sous-montants dont le total est égal audit montant transactionnel. Les sous-montants sont fonction du secret partagé entre l'institution de paiement, par exemple une banque, et le moyen de paiement, par exemple une carte bancaire. Le destinataire du paiement peut alors vérifier que le découpage en sous-montants est conforme au secret et au montant, et ainsi s'assurer de l'authenticité de la transaction.

Par ailleurs, les sous-montants obtenus selon la présente invention sont très difficilement identifiables par un tiers sans la connaissance de l'information secrète et des algorithmes de

détermination de ces sous-montants, et la sécurité de la transaction en est améliorée.

Par ailleurs, afin que, pour un même montant transactionnel, les sous-montants soient différents d'une transaction à une autre, il est avantageux de prendre en compte un identifiant de chaque transaction dans le calcul des sous-montants.

Le procédé selon l'invention peut donc comprendre en outre de l'étape de transmission dudit montant transactionnel, une étape de transmission d'un identifiant de ladite transaction ; ladite valeur de codage transactionnelle étant en outre fonction dudit identifiant, ladite institution de paiement authentifiant ladite transaction en outre en fonction dudit identifiant.

Un exemple simple de tel identifiant de transaction est la date et/ou l'heure de la transaction. Une précision donnée sur la date et l'heure, par exemple d'une seconde, empêchera alors la génération des mêmes sous-montants pour le même montant transactionnel selon deux transactions espacées de plus d'une seconde.

Afin que la valeur de codage transactionnelle calculée ne puisse être déterminée facilement par un tiers, la génération de ladite valeur de codage transactionnelle au moins en fonction dudit montant transactionnel et de ladite première information secrète dépend d'une fonction de calcul apte à générer des nombres pseudo-aléatoires en fonction dudit montant transactionnel et de ladite première information secrète.

De la même façon, afin de rendre difficile la détermination de ladite valeur de codage transactionnelle par un tiers par essais successifs sur une liste exhaustive d'informations secrètes, ladite

première information secrète est par exemple un nombre long, typiquement d'au moins 8 octets.

L'invention a également pour objet un moyen de paiement comprenant au moins un processeur et une mémoire stockant une première information secrète partagée avec une institution de paiement, ledit moyen de paiement étant apte à recevoir un montant transactionnel depuis un terminal de lecture, ce moyen de paiement comprenant des moyens pour générer à l'aide dudit processeur, au moins une valeur de codage transactionnelle, ladite valeur de codage transactionnelle étant au moins fonction dudit montant transactionnel et de ladite première information secrète.

Le moyen de paiement est adapté au terminal de lecture utilisé. En particulier, le moyen de paiement peut être une carte bancaire, et le terminal de lecture, un lecteur de carte tel que décrit précédemment. Le moyen de paiement peut également être une carte apte à être insérée dans un téléphone mobile, par exemple une carte UICC, et le terminal de lecture est dans ce cas le téléphone mobile lui-même.

Le terminal de lecture comprend de préférence une interface homme-machine sous la forme d'un écran et d'un clavier, l'écran du terminal pouvant être utilisé pour afficher à l'utilisateur les sous-montants calculés selon le procédé ci-dessus mentionné, et le clavier pouvant être utilisé pour que l'utilisateur saisisse le montant transactionnel.

Par exemple, pour l'achat par Internet d'un produit sur un site donné, le site fournit à l'utilisateur le prix du produit, l'utilisateur entre le prix au niveau du terminal de lecture et insère sa carte bancaire dans le terminal de lecture, le terminal de lecture transmet le prix à la carte bancaire, la carte bancaire calcule les sous-

montants à partir du montant et de la clé secrète, le terminal de lecture affiche les sous-montants, et l'utilisateur paie alors au site le prix sous la forme de plusieurs sous-transactions correspondant aux sous-montants. Le site transmet alors les sous-montants à la banque associée à la carte bancaire, qui, à l'aide du prix total correspondant à la somme des sous-montants, et de l'information secrète associée à la carte, authentifie la transaction.

L'invention a également pour objet un programme d'ordinateur destiné à la mise en œuvre du procédé sus mentionné, ce programme comprenant une pluralité d'instructions pour générer au moins une valeur de codage transactionnelle, ladite valeur de codage transactionnelle étant au moins fonction dudit montant transactionnel et de ladite première information secrète.

D'autres buts et avantages de la présente invention apparaîtront à la lecture de la description de ses modes de réalisation.

L'invention sera également mieux comprise à l'aide des dessins, dans lesquels :

- La figure 1 est un exemple de diagramme schématique du procédé mis en œuvre selon la présente invention ;
- La figure 2 est un exemple de diagramme bloc du procédé mis en œuvre selon la présente invention.

La figure 1 décrit un exemple de réalisation de l'invention dans le cas d'une transaction par Internet depuis un poste utilisateur de type ordinateur.

Selon l'invention, on réalise une transaction à partir d'un moyen de paiement, par exemple sous la forme d'une carte bancaire 1 comprenant un processeur apte à réaliser des calculs, une

mémoire non volatile apte à stocker des données, une mémoire RAM et une mémoire de type E2PROM ou Flash.

La carte bancaire 1 peut interagir avec un terminal de lecture 2. Ce terminal peut transmettre des données à la carte, recevoir des données en provenance de la carte, et alimenter la carte électriquement. Il comprend également un clavier et un écran pour saisir et afficher des informations.

Le terminal de lecture 2 est connecté à un poste utilisateur sous la forme d'un ordinateur 3.

Dans l'exemple d'un achat sur Internet, l'utilisateur désire acheter un produit auprès d'un vendeur 4 matérialisé par un site marchand transmettant ses offres sur le poste 3. De façon connue en soi, lorsque l'utilisateur réalise un achat sur Internet, il fournit les données de sa carte sous la forme d'un numéro de carte et d'une date d'expiration, et le site transmet ensuite ces données ainsi que le montant payé à la banque 5 afin que celle-ci réalise la transaction après authentification des données de la carte.

La figure 2 décrit plus en détail le procédé selon l'invention. La carte 1 contient dans sa mémoire non volatile E2PROM ou flash, une information secrète K. Cette information est secrète au sens où elle n'est partagée qu'entre la banque 5 et la carte 1, l'utilisateur n'ayant pas connaissance de cette clé K. En pratique, une telle clé est insérée en mémoire au moment de la fabrication de la carte 1 dans des locaux hautement sécurisés. Cette clé K est associée à un numéro de série de la carte. La banque peut par exemple retrouver la relation entre le numéro de série et la clé à partir d'une base de données mettant en relation les numéros de série des cartes et les clés secrètes. La clé K peut aussi être générée aléatoirement ou plus avantageusement dérivée d'une clef mère Km par un des

mécanismes connus dans le domaine, évitant ainsi à la partie qui effectue la vérification de stocker toutes les clés de toutes les cartes. La clé mère Km sert, lors d'une vérification, à régénérer la clé K de la carte correspondant à la transaction à traiter. De façon plus générale, la banque possède les moyens de retrouver la clé secrète d'une carte par exemple à partir de son numéro de série.

La carte 1 comprend également en mémoire un programme d'ordinateur implémentant un algorithme de calcul ALG qui peut être mis en œuvre à l'aide du processeur de cette carte. Cet algorithme ALG peut prendre en données d'entrée des données stockées en mémoire de la carte 1, ou reçues par la carte 1.

Selon l'invention, lorsque l'utilisateur décide de faire un achat pour un montant A, par exemple de 100 Euros, il entre le montant de 100 Euros au niveau du terminal de lecture 2, par exemple par l'intermédiaire du clavier du terminal. Il insère également sa carte 1 dans le terminal de lecture 2.

Le terminal de lecture transmet ensuite le montant A (en étape 10) à la carte 1, ainsi que la date et l'heure associée à la transaction D. On note que la date et l'heure de la transmission peuvent être par exemple connues par le lecteur qui comprend une fonction d'horloge, ou elles peuvent être transmises au lecteur par l'utilisateur ou par un dispositif d'horloge associé au lecteur.

À réception de ces données, la carte calcule (en étape 20), à l'aide de son processeur, une pluralité de sous-montants A_i en appliquant l'algorithme ALG avec en données d'entrée, A, K, et D. On a donc A_i=ALG (A, K, D), i=1 à N, N étant déterminé par l'algorithme ALG.

Les sous-montants A_i sont tels que la somme de A_i est égale au montant A, soit $A = \sum_{1}^{N} A_i$.

Les sous-montants A_i sont ensuite transmis (en étape 30) à l'utilisateur, par exemple par l'intermédiaire de l'écran du terminal de lecture.

L'utilisateur paie ensuite le produit sur le site marchand 4 en une pluralité de sous-transactions T_i, chacune des sous-transactions $T_é$ correspondant au montant A_i. Il transmet également un identifiant de sa carte bancaire 1, par exemple sous la forme d'un numéro de carte et d'une date d'expiration de la carte.

Afin d'être payé du montant A pour l'achat d'un produit, le site marchand 4 transmet alors (en étape 40) l'identifiant de la carte bancaire 1 à la banque 5, ainsi que tous les montants A_i correspondant aux transactions $T_é$ ayant la même date et heure.

À l'aide de l'identifiant de la carte 1, la banque 5 retrouve la clé K' associée à cet identifiant. La banque a également connaissance de l'algorithme ALG ayant servi à calculer les sous-montants A_i pour une date D.

La banque 5 fait alors la somme de tous les sous-montants reçus pour une même transaction issue de la carte 1. Elle retrouve donc (en étape 50) le montant total de la transaction A.

Elle calcule alors des sous-montants A'_i=ALG (K',A,D). Si les sous-montants A'_i sont égaux aux sous-montants A_i, c'est que la clé secrète K' récupérée par la banque 5 correspond bien à la clé secrète K de la carte ayant servie à la transaction. Dans ce cas, la banque 5 authentifie (en étape 60) la transaction et valide le paiement du site 4. En effet, le fait que la banque ait retrouvé

l'ensemble des sous-montants Ai indique que l'algorithme ayant permis de générer les sous-montants Ai a été réalisé par la carte stockant la clé K.

Si un tiers mal intentionné était en possession de la carte bancaire 1 et désirait réaliser des transactions par Internet, il paierait directement pour le montant A. Ceci serait alors interprété par la banque comme un sous-montant tel que A_i=A, i=1, et elle calculerait alors A'_i=ALG (K',A,D), K' étant la clé secrète de la carte ayant servie à la transaction, et la probabilité est très faible pour que ce calcul redonne A_i=A, i=1. La transaction ne serait alors pas authentifiée et le paiement refusé, ou bien la transaction deviendrait répudiable.

Par ailleurs, un tiers mal intentionné qui calculerait les sous-montants Ai pour un montant A donné sans posséder la clé K aurait une probabilité négligeable de retrouver le bon découpage en sous-montants Ai.

Nous décrivons maintenant plus en détail l'algorithme ALG utilisé conformément à la présente invention. Cet algorithme ALG prend en données d'entrée, un montant transactionnel A, l'heure et la date de la transaction D, et le secret partagé par la carte et la banque 5.

Selon l'algorithme ALG, on calcule d'abord un nombre pseudo-aléatoire S, à l'aide d'une fonction R. Cette fonction est de préférence à sens unique (fonction « one way » en langue anglaise), et sans collision. Un exemple de telle fonction est la fonction connue en cryptographie HMAC-SHA2. Avec une telle fonction, on peut calculer un nombre pseudo-aléatoire S possédant jusqu'à 512 bits. Si ceci n'est pas suffisant, on peut encore itérer la fonction R sur le nombre S obtenu. Un autre exemple de fonction R pourrait

être à base de DES afin de profiter de la présence d'un composant dédié dans certaines cartes à puces 1 et donc d'accélérer les calculs cryptographiques.

Le nombre pseudo-aléatoire S ayant été calculé, on génère ensuite les N sous-montants A_i à l'aide d'une fonction F prenant S et A comme argument, de sorte que $A = \sum_{1}^{N} A_i$.

Le nombre N est déterminé par la fonction F selon le montant A et de sorte que la probabilité d'obtenir deux fois le même ensemble de sous-montants soit très faible.

Par exemple, si l'on considère la suite stochastique d'entiers correspondant à l'événement « A est découpé en N sous-montants dont la somme est égale à A », on peut choisir F tel que la probabilité d'obtenir le même découpage est inférieure par exemple à 2^{-50}.

On peut par exemple définir F comme

$$F:(S,A)\mapsto \begin{cases} A_1 = S \bmod 2^k, \\ A_2 = \left[\frac{S}{2^k}\right] \bmod 2^k \\ \cdots \\ A_{n-1} = \left[\frac{\ddot{S}}{2^{(n-2)k}}\right] \bmod 2^k \\ A_n = A - \sum_{1}^{n-1} A_i, \text{ tel que } A_n \in \left[\frac{A}{n} - (n-1).\varepsilon, A\right] \end{cases}$$

avec k tel que $A_i \in \left[0; \frac{A}{n} + \varepsilon\right]$ pour $1 \le i \le n-1$, ε étant adapté pour le nombre de bits.

Ainsi, si l'utilisateur désire payer 100 Euros, soit 10 000 centimes, par téléphone ou par Internet, on choisit A= 10000 et par exemple pour n=10,

$$\forall i, i \in [1;9] \quad A_i \in [0;1024] \; A_i = \left[\frac{S}{2^{10.(i-1)}}\right] \bmod 2^{10} \quad \text{and } A_{10} \in [784;10000]$$

avec ici k=10, 2^{10}=1024 et ε=24.

On considère maintenant une attaque possible du procédé selon l'invention consistant à générer, pour un montant donné A, tous les ensembles de sous-montants possibles afin d'obtenir le bon découpage. Dans ce cas, pour la fonction F décrite ci-dessus, les n-1 premiers sous-montants sont issus de la source pseudo-aléatoire S=R(A,D,K). La probabilité que pour une date et heure D fixée, quelqu'un trouve le bon découpage est alors :

$$P = \frac{1}{\left(\frac{A}{n} + \varepsilon + 1\right)^{n-1}}.$$

On note qu'un avantage de ce mode de réalisation est que, pour un nombre de montants donné, la probabilité de retrouver le bon découpage diminue lorsque le montant transactionnel A augmente. Le procédé est donc d'autant plus sécurisé que le montant à payer est élevé. De plus, pour une probabilité P fixée d'avoir le même ensemble de sous-montants, le nombre n de sous-montants diminue lorsque le montant transactionnel augmente.

Ainsi, l'attaque consistant à générer $\left(\frac{A}{n} + \varepsilon + 1\right)^{n-1}$ combinaisons différentes devient très difficile si n est choisi convenablement en fonction du montant A.

Dans l'exemple ci-dessus, la probabilité de retrouver le bon découpage est de $\left(\frac{1}{(1025)}\right)^9 \cong 2^{-90}$.

Afin d'avoir une probabilité de retrouver le bon découpage jugée satisfaisante, on peut donc choisir 10 sous-montants pour un montant total de 100 Euros, et seulement 5 sous-montants pour un montant total de 10000 Euros.

Nous avons décrit ci-dessus un mode de réalisation de l'invention dans lequel le montant transactionnel est découpé en sous-montants A_i tels que la somme des A_i est égale au montant transactionnel A. Selon l'invention, on prévoit aussi que les sous-montants A_i ne soient pas nécessairement de somme égale au montant transactionnel A.

En effet, le n-uplet $(A_1, ..., A_n)$ est calculé à partir d'une fonction F prenant en paramètre au moins le montant transactionnel A et la clé K. Si la fonction F est partiellement inversible, c'est-à-dire si on peut retrouver A à partir de la clé K et du n-uplet $(A_1, ..., A_n)$, alors la banque pourra calculer le montant transactionnel A, refaire le calcul pour déterminer le n-uplet $(A_1, ..., A_n)$, et donc authentifier ou non la transaction, même si la somme des A_i n'est pas égale à A.

On comprend dans ce cas que les variables A_i correspondent plus généralement à un codage transactionnel du montant transactionnel A, le codage transactionnel ayant la forme d'un n-uplet, la clé de codage étant constitué par la clé K et la fonction F tel que : $F(A,K)=(A_1, A_2, ..., A_n)$.

La façon dont est réalisée le codage transactionnel du montant transactionnel peut alors permettre de maîtriser le niveau de sécurité de la transaction.

Par exemple, en reprenant les nombres aléatoires A_1, A_2 et A_3 tels que précédemment décrits pour n=3, on peut transmettre non pas les sous-montants A_i, mais les valeurs de codage transactionnelles suivantes:

T_1= (A XOR A1 XOR A2)

T_2= A1

T_3= A2

Dans ce cas, le montant transactionnel peut être recalculé par la banque par le calcul T_1 XOR T_2 XOR T_3, et la transaction peut donc être identifiée.

Dans le cas particulier où la somme des A_i est égale au montant transactionnel A, les valeurs de codage transactionnelles du montant transactionnel correspondent à des sous-montants du montant transactionnel A.

On décrit maintenant différentes variantes avantageuses du procédé selon l'invention.

Selon une première de ces variantes, après authentification de la transaction par la banque 5 destinataire, celle-ci peut substituer aux n sous-transactions une seule transaction reconstituée afin d'éviter de provoquer la confusion sur les relevés de comptes du porteur de la carte 1 ainsi que des coûts de traitement supplémentaires. Le porteur de la carte 1 verra donc sur son relevé de compte le montant A correspondant au produit acheté et non les n sous-montants A_i.

Selon une autre de ces variantes, l'utilisateur peut vérifier sa propre transaction à l'aide de sa carte 1 lorsqu'il reçoit un relevé de compte mentionnant une pluralité de sous-montants correspondant à une date et à une heure donnée. Cette vérification peut également être faite de façon automatique si le relevé de compte est sous format électronique. Dans ce cas, la carte insérée dans un lecteur recalcule les sous-montants correspondant au montant transactionnel A et authentifie sa propre transaction comme le fait la banque selon le procédé de l'invention. Ceci peut par exemple être réalisé sur un lecteur indépendant de type GemPocket connu.

Dans le cas où la date et/ou l'heure sont prises en compte dans le calcul des sous-montants, l'utilisateur peut également entrer la date de la transaction telle qu'elle apparaît sur son relevé de compte au niveau du lecteur de carte afin de retrouver les sous-montants.

Il est entendu que les algorithmes mis en œuvre par la présente invention et en particulier l'algorithme ALG embarqué dans la carte 1 peuvent être embarqués sur celle-ci en complément d'une autre application, par exemple une application de débit crédit de type EMV. Les applications embarquées correspondant à la mise en oeuvre de la présente invention peuvent également être les seules applications embarquées dans la carte. Dans le cas où l'invention cohabiterait sur la carte avec une autre application, les applications peuvent être totalement séparées ou collaborer et/ou partager des données et/ou des fonctions de base telles que des algorithmes cryptographiques, ou des fonctions de hachage.

Selon un mode de réalisation particulier, la clé K peut donc être la clef secrète d'une application de débit/crédit embarquée sur la carte 1, ce qui évite ainsi de gérer une clef supplémentaire dans la carte 1.

Par ailleurs, nous avons décrit un exemple dans lequel c'est la banque 5 qui réalise l'authentification de la transaction à partir des sous-montants A_i, mais il est entendu que cette étape d'authentification peut être réalisée par une autre entité que la banque, la banque ne recevant alors que le résultat de l'authentification. Aux fins de la présente invention, l'institution de paiement correspond donc à la banque, éventuellement associée à des entités traitant l'authentification, ou bien à ces entités seules.

Enfin, dans le cas d'une transaction Internet, et si le lecteur 2 peut être piloté par le terminal 3 connecté à Internet, on peut implémenter sur le terminal un logiciel qui effectue automatiquement les tâches de communication du montant de la transaction et de la date à la carte 1, de récupération des sous-montants et de remplissage d'un formulaire Web avec les sous-montants.

Le moyen de paiement selon l'invention peut être une carte à puce fonctionnant en mode contact ou sans contact, nécessitant la saisie d'un code PIN ou non. Le moyen de paiement peut également être un ordinateur stockant une clé secrète K, ou une carte UICC comprenant une application apte à mettre en œuvre la présente invention.

Le terminal de lecture peut être tout terminal apte à recevoir les données du moyen de paiement. Il peut être relié à un ordinateur ou compris dans l'ordinateur dans le cas d'un lecteur intégré. On note que dans le cas d'un lecteur intégré, les sous-montants A_i peuvent être transmis directement dans un formulaire d'achat ou à la banque de façon transparente pour l'utilisateur.

Il peut également être un terminal mobile de type téléphone mobile, un téléphone fixe, combiné ou non à un minitel muni d'un lecteur de carte.

La saisie des sous-montants par l'utilisateur pour la réalisation de la transaction peut être réalisée à l'aide d'un clavier, correspondant par exemple aux touches d'un ordinateur, d'un téléphone ou d'un minitel, ou de vive voix par exemple pour un paiement ou une réservation par téléphone.

Les différentes variantes ci-dessus peuvent bien sûr être utilisées en combinaison afin de mettre en œuvre l'invention.

REVENDICATIONS

1. Procédé pour réaliser une transaction d'un montant transactionnel (A) entre un moyen de paiement (1) et une institution de paiement (5) par l'intermédiaire d'un terminal de lecture (2), ledit moyen de paiement (1) comprenant au moins un processeur et une mémoire stockant une première information secrète (K) partagée avec ladite institution de paiement (5), ledit terminal de lecture (2) étant apte à transmettre des données audit moyen de paiement, le procédé étant caractérisé en ce qu'il comprend les étapes :

- de transmission (10) par ledit terminal de lecture (2), audit moyen de paiement (1), d'au moins ledit montant transactionnel (A);
- de génération (20) par ledit moyen de paiement (1), à l'aide dudit processeur, d'au moins une valeur de codage transactionnelle, ladite valeur de codage transactionnelle étant au moins fonction dudit montant transactionnel (A) et de ladite première information secrète (K) ;
- de transmission (40) dudit codage transactionnel à ladite institution de paiement;
- d'authentification (50, 60) par ladite institution de paiement, de ladite transaction correspondant audit montant transactionnel en fonction dudit codage transactionnel et de ladite première information secrète (K).

2. Procédé pour réaliser une transaction selon la revendication 1, comprenant les étapes de transmission par ledit terminal de lecture audit moyen de paiement, en outre dudit montant transactionnel A, d'un identifiant de ladite transaction, ladite valeur de codage transactionnel étant en outre fonction dudit identifiant, ladite institution de paiement, authentifiant ladite transaction en outre en fonction dudit identifiant.

3. Procédé pour réaliser une transaction selon la revendication 2, dans lequel ledit identifiant est au moins la date et l'heure (D) de ladite transaction.

4. Procédé pour réaliser une transaction selon l'une des revendications 1 à 3, dans lequel la génération de ladite valeur transactionnel au moins en fonction (R) dudit montant transactionnel et de ladite première information secrète dépend d'une fonction de calcul apte à générer au moins un nombre pseudo-aléatoire (S) en fonction dudit montant transactionnel et de ladite première information secrète.

5. Procédé pour réaliser une transaction selon l'une des revendications 1 à 4, dans lequel ladite valeur de codage transactionnelle correspond à au moins un sous-montant, la somme desdits sous-montants étant égale audit montant transactionnel.

6. Procédé pour réaliser une transaction selon l'une des revendications 1 à 5, dans lequel ledit moyen de paiement est une carte à puce et dans lequel ledit terminal de lecture est un lecteur de carte à puce.

7. Moyen de paiement (1) comprenant au moins un processeur et une mémoire stockant une première information secrète (K) partagée avec une institution de paiement (5), ledit moyen de paiement (1), étant apte à recevoir un montant transactionnel (A) depuis un terminal de lecture (2), caractérisé en ce qu'il comprend des moyens pour générer, à l'aide dudit processeur, au moins une valeur de codage transactionnelle au moins fonction dudit montant transactionnel et de ladite première information secrète.

8. Moyen de paiement selon la revendication 7, dans lequel ladite au moins une valeur de codage transactionnelle correspond à au moins un sous-montant, la somme desdits sous-montants étant égale audit montant transactionnel.

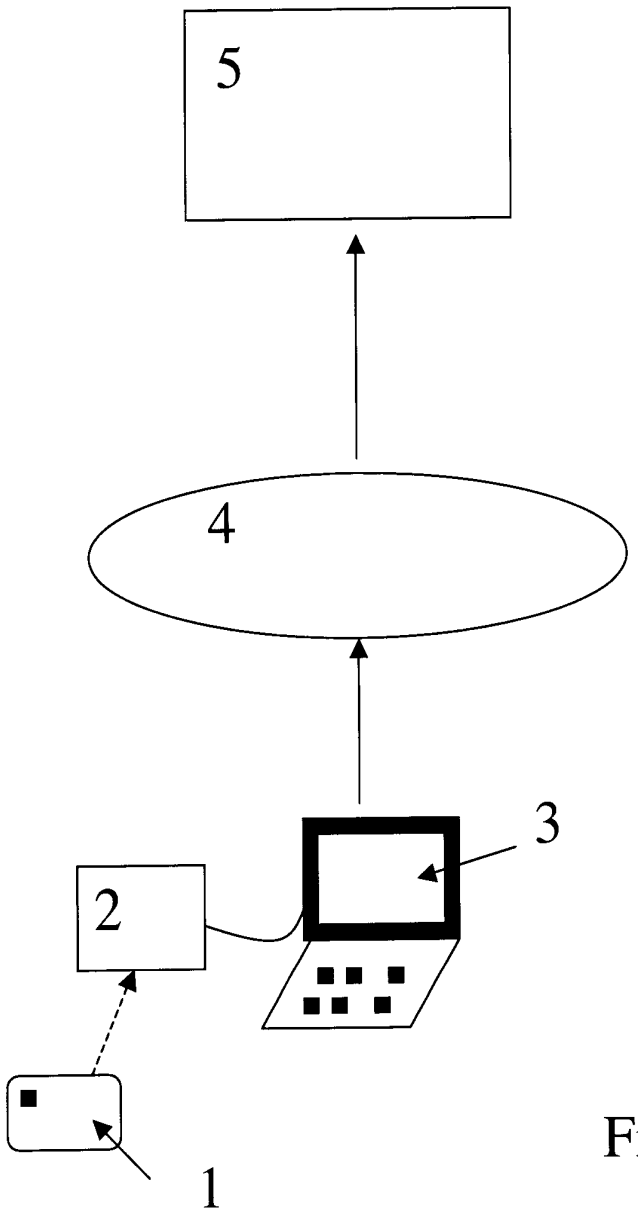


Figure 1

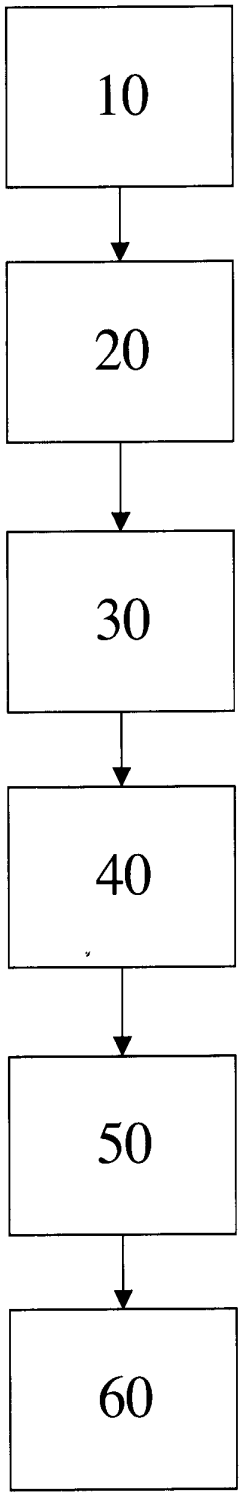


Figure 2

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 672679
FR 0511081

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 2002/016913 A1 (WHEELER LYNN HENRY ET AL) 7 février 2002 (2002-02-07) * abrégé * * alinéas [0318] - [0332]; figure 28 * * alinéas [0371] - [0379]; figure 33 * * alinéa [0387] * * alinéa [0412] *	1-8	H04L9/14 G06F7/58
X	"SET SECURE ELECTRONIC TRANSACTION SPECIFICATION BOOK 1: BUSINESS DESCRIPTION" SET SECURE ELECTRONIC TRANSACTION SPECIFICATION, XX, XX, 31 mai 1997 (1997-05-31), pages I-V,1, XP001051175 * alinéa [04.4] *	1-8	
A	ABADI ET AL: "Authentication and Delegation with Smart-cards" 22 octobre 1990 (1990-10-22), SRC RESEARCH REPORT, PAGE(S) 1-25 , XP002137406 * alinéas [0003], [0004] *	1-8	DOMAINES TECHNIQUES RECHERCHÉS (IPC) G06Q
A	TATSUAKI OKAMOTO ED - COPPERSMITH D (ED) INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH: "AN EFFICIENT DIVISIBLE ELECTRONIC CASH SCHEME" ADVANCES IN CRYPTOLOGY - CRYPTO '95. SANTA BARBARA, AUG. 27 - 31, 1995, PROCEEDINGS OF THE ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE (CRYPTO), BERLIN, SPRINGER, DE, vol. CONF. 15, 27 août 1995 (1995-08-27), pages 438-451, XP000565124 ISBN: 3-540-60221-6 * le document en entier *	5,8	

-/--

Date d'achèvement de la recherche	Examinateur
26 avril 2006	Dedek, F

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

1

EPO FORM 1503 12.99 (P04C14)

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 672679
FR 0511081

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		
A	MING ZHONG ET AL: "Single-term divisible electronic cash based on bit commitment" COMPUTERS AND COMMUNICATIONS, 2000. PROCEEDINGS. ISCC 2000. FIFTH IEEE SYMPOSIUM ON JULY 3-6, 2000, PISCATAWAY, NJ, USA,IEEE, 3 juillet 2000 (2000-07-03), pages 280-285, XP010505359 ISBN: 0-7695-0722-0 * le document en entier * -----	5,8	

DOMAINES TECHNIQUES RECHERCHÉS (IPC)

Date d'achèvement de la recherche	Examinateur
26 avril 2006	Dedek, F

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

1

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0511081 FA 672679

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 26-04-2006
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 2002016913 A1	07-02-2002	AUCUN	

EPO FORM P0465