(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 043 871**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **15 02412**

(51) Int Cl[8] : ***H 04 L 9/32*** *(2017.01), G 06 K 19/077*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 16.11.15.

(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) :** *LAZZARI MYRIAM* — FR.

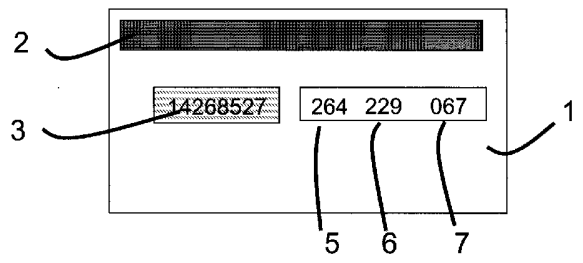
(72) **Inventeur(s) :** LAZZARI MYRIAM et LAZZARI BAPTISTE.

(73) **Titulaire(s) :** LAZZARI MYRIAM.

(74) **Mandataire(s) :** LAZZARI MYRIAM.

(54) PROCEDE DE SECURISATION PAR CARTE BANCAIRE DES TRANSACTIONS EN LIGNE PAR TELEPHONE OU FAX.

(57) L'invention concerne le domaine de la sécurisation des transactions en ligne, par internet téléphone, ou fax, ou tout autre moyen nécessitant la divulgation des données sécuritaires, à partir d'une carte bancaire de crédit ou de débit, associée à un compte bancaire. L'invention a pour but de sécuriser le code de sécurité généralement inscrit sur la face arrière de la carte, souvent appelé cryptogramme. Plusieurs cryptogrammes sont inscrits sur la carte bancaire, et son reconnus par la banque. Le même cryptogramme ne peut pas être utilisé pour deux transactions consécutives.



FR 3 043 871 - A1

PROCEDE DE SECURISATION PAR CARTE BANCAIRE, DES TRANSACTIONS EN LIGNE PAR TELEPHONE OU FAX.

DESCRIPTIF

Domaine d'application de l'invention

La présente invention concerne un procédé de sécurisation par carte bancaire, des transactions en ligne par téléphone ou fax. Elle concerne le domaine de la sécurisation des transactions par internet, téléphone ou fax à partir d'une carte bancaire de crédit ou de débit, associée à un compte bancaire. L'invention a pour but de sécuriser le code de sécurité généralement inscrit sur la face arrière de la carte, souvent appelé cryptogramme.

Etat de l'art antérieur

Le commerce en ligne (internet, téléphone ou fax), utilisant les cartes bancaires, s'est considérablement développé. Malheureusement, en même temps les fraudes par piratage des données sécurisées du propriétaire de la carte se sont également généralisées. On estime actuellement que plus de 60% des fraudes à la carte bancaire, viennent du piratage en ligne des données personnelles du propriétaire de la carte. Ces données personnelles comprennent généralement, un numéro de carte, le nom et prénom du propriétaire, la date d'expiration de la carte qui sont souvent « embossées » sur la face avant de la carte.
Sur la face arrière, se trouve inscrit un code, à trois ou quatre chiffres, le cryptogramme. Le

piratage de ces données en ligne, permet au pirate de commander en ligne des objets, qu'il se fera livrer à une adresse nomade ou éphémère.

De nombreux dispositifs ont été développés pour tenter de mieux sécuriser les données des cartes bancaires, notamment le cryptogramme.

Le brevet US2013061057, propose l'utilisation d'un téléphone cellulaire, associé à la carte, qui par les codes de sécurité du téléphone, améliore celle de la carte.

Le brevet US2012280048 propose l'insertion d'une antenne RFID dans la carte, qui par sa liaison à un serveur local, sécurise la transaction.

Le brevet US2010299267, décrit un cryptage du cryptogramme, par l'intermédiaire d'un processeur, lié à une carte à puce, ou à un ordinateur.

Le brevet US2011272472 propose un émulateur magnétique qui à partir de la piste magnétique de la carte, permet de changer périodiquement le cryptogramme.

Les brevets US2012325905, US2010127083, EP2568448, proposent l'insertion dans la carte bancaire d'un écran affichant le cryptogramme, qui peut être modifié séquentiellement par une électronique insérée dans la carte, en coordination avec la banque, sans liaison directe.

Si ces inventions sont intéressantes à certains égards, elles sont complexes, font appel à de l'électronique extérieure, et s'agissant de dispositif encastrés dans la carte, avec des écrans affichant les cryptogrammes, sont très chères, et peuvent présenter des problèmes de fiabilité. Par

ailleurs, la périodicité des changements de cryptogrammes, permet durant la validité du cryptogramme d'effectuer des transactions frauduleuses.

Exposé de l'invention

La présente invention a pour but de remédier aux inconvénients de l'art antérieur, pour sécuriser les transaction utilisant une carte bancaire, lorsque cette transaction nécessite la divulgation des données sécuritaires, comme le numéro de carte, le nom, et prénom du propriétaire, la date d'expiration de la carte, et le cryptogramme, divulgation qui peut se faire notamment par internet, téléphone ou fax, ou tout autre moyen. L'invention concerne plus particulièrement la sécurisation du cryptogramme. L'invention propose l'inscription par la banque de plusieurs cryptogrammes différents sur la carte, chaque cryptogramme étant reconnu par celle-ci. Pour effectuer une transaction, le propriétaire de la carte divulgue en ligne ou par téléphone, ou faxe, ou tout autre moyen, son numéro de carte, son nom, son prénom, la date d'expiration de la carte, et un des cryptogrammes inscrits sur la carte. La sécurisation des transactions, s'effectue par le refus de la banque d'une seconde transaction consécutive à la première transaction, utilisant le même cryptogramme. Une nouvelle transaction consécutive à la première, doit utiliser un ou plusieurs des autres cryptogrammes inscrits sur la carte bancaire, avant de pouvoir réutiliser le cryptogramme de la précédente transaction.

De façon plus précise, l'invention a pour objet un procédé de sécurisation des transactions par carte bancaire, associée à un compte bancaire, en ligne par téléphone ou fax, ou tout autre moyen nécessitant la divulgation des données sécuritaires, comportant le numéro de la carte bancaire, le nom et le prénom du propriétaire, la date d'expiration de la carte. Plusieurs cryptogrammes, différents sont inscrits sur la carte, et reconnus par la banque. Après une transaction utilisant un de ces cryptogrammes, divulgué par le propriétaire pour effectuer sa transaction, la banque n'accepte plus l'utilisation de ce même cryptogramme pour la transaction suivante. Ce même cryptogramme ne pouvant être accepté par la banque qu'après que le propriétaire ait effectué au moins une autre transaction utilisant au moins un autre cryptogramme inscrit sur la carte.

Les transactions selon l'invention, peuvent s'effectuer par internet, par téléphone ou faxe, ou tout autre moyen nécessitant la divulgation des informations sécuritaires, notamment du cryptogramme.

Lors d'une transaction (T1), visant par exemple l'achat en ligne d'un objet, le propriétaire de la carte bancaire, divulgue par internet au site du vendeur, les informations contenues sur sa carte, soit son numéro de carte, son nom, son prénom, la date d'expiration, et un des cryptogrammes (C1) inscrits sur sa carte. Ces données étant reconnues par la banque, celle-ci autorise la transaction (T1). Au cours ou à la suite de cette transaction (T1) si un piratage des données intervenait, le pirate

utilise les mêmes données pour faire par exemple, un achat frauduleux. La banque interdit alors immédiatement cette transaction frauduleuse, car le même cryptogramme (C1) aura été utilisé deux fois de suite pour deux transactions consécutives.

Le propriétaire de la carte peut effectuer une autre transaction (T2) en utilisant un autre cryptogramme (C2) inscrit sur sa carte. Cette seconde transaction est acceptée par la banque. S'il devait faire une troisième transaction (T3) il pourrait réutiliser le premier cryptogramme (C1), selon un premier mode de l'invention.

Selon un second mode de l'invention, plusieurs transactions avec des cryptogrammes différents, sont nécessaire pour pouvoir réutiliser le même cryptogramme. Ce nombre de transaction est défini par la banque.

Selon un troisième mode de l'invention, l'utilisation des cryptogrammes se fait dans un ordre déterminé prédéfini par la banque.

Selon un quatrième mode de l'invention, un ou plusieurs des cryptogrammes inscrit sur la carte, est interdit à l'utilisation. Ces cryptogrammes sont choisis par la banque qui en informe le propriétaire de la carte.

Les modes trois et quatre selon l'invention, peuvent être utilisés séparément ou en combinaison entre eux.

Si le propriétaire de la carte engage par erreur une seconde transaction selon le premier mode de l'invention par exemple, (suite à une première

transaction), avec le même cryptogramme, la transaction est bloquée par la banque. Le propriétaire détecte vite son erreur car il est informé que sa transaction a été bloquée. Il peut alors déclarer son erreur à sa banque, par un contact téléphonique ou un SMS. La banque qui est à l'origine du blocage, peut à l'inverse, si elle n'a pas reçu d'information du propriétaire, contacter le propriétaire, pour vérifier s'il s'agit d'une erreur de sa part ou non.

S'il ne s'agit pas d'une erreur du propriétaire, la banque sait immédiatement qu'elle a affaire à une tentative de piratage.

Elle peut donc engager sans attendre une recherche, afin de reconstituer la traçabilité de cette tentative de piratage, car l'ayant immédiatement détectée, elle peut remonter à sa source, plus facilement, alors que selon l'art antérieur, avec un seul cryptogramme, c'est souvent le propriétaire qui détecte la fraude, en consultant ses relevés bancaires, parmi un ensemble de transactions non frauduleuses qu'il a accomplies, c'est-à-dire bien après que la fraude se soit produite. Il arrive même qu'il ne s'en aperçoive pas, si le montant de la fraude n'est pas très élevé.

Cette instantanéité de détection des tentatives de piratage, est un avantage important du procédé selon l'invention, car non seulement il évite la fraude, mais en plus il contribue à son éradication par la recherche immédiate de l'auteur de la tentative de fraude.

Présentation des figures

D'autres données, caractéristiques et avantages de la présente invention apparaîtront à la lecture de la description détaillée non limitative qui suit, en référence aux figures annexées qui représentent, respectivement :

- la figure 1, un exemple de l'art antérieur
- la figure 2, la vue arrière d'une carte de paiement selon l'invention.

Description détaillée

La figure 1 représente la face arrière d'une carte de bancaire 1 selon l'art antérieur. La piste magnétique 2 se trouve généralement au bord supérieur de la face arrière de la carte bancaire. Un code 3 plus ou moins masqué par des impressions colorées, superposées au code, n'est pas utilisé pour les transactions en ligne, seul le code 4 généralement composé de 3 chiffres, que l'on nomme souvent cryptogramme, est utilisé, en complément du numéro de carte, du nom et prénom du propriétaire, ainsi que la date d'expiration de la carte qui se trouvent sur la face avant de la carte. Ces informations sont divulguées en ligne ou par téléphone au vendeur.

La figure 2 montre la face arrière 1 d'une carte bancaire selon l'invention.

La piste magnétique 2, et le code 3 sont déjà décrrit à la figure 1. La carte comporte selon l'exemple de la figure 2, trois cryptogrammes 5, 6, et 7. Chaque cryptogramme a un code différent. Le propriétaire de

la carte, peut divulguer en ligne, (en complément du numéro de carte, de son nom, de son prénom, et de la date d'expiration de sa carte), un de ces trois cryptogrammes pour effectuer un achat en ligne par exemple le cryptogramme 5. Pour une transaction suivante, il peut utiliser soit le cryptogramme 6 ou le cryptogramme 7. Selon le premier mode de l'invention, pour une troisième transaction, il peut de nouveau utiliser le cryptogramme 5.

Selon le second mode de l'invention, il ne peut utiliser le cryptogramme 5 qu'après avoir utilisé les cryptogrammes 6 et 7.

Selon le troisième mode de l'invention, le propriétaire doit utiliser dans l'ordre les cryptogrammes 5, puis 6, puis 7 pour effectuer trois transactions, puis la même séquence se renouvelle pour les transactions suivantes.

Le nombre de cryptogrammes selon l'invention, n'est pas limité, seule la taille de l'impression des cryptogrammes, par rapport à la surface disponible en face arrière, limite le nombre de cryptogrammes. D'une façon pratique, le nombre de cryptogrammes peut être par exemple compris entre trois et dix.

Parmi ces cryptogrammes il est proposé selon l'invention, d'avoir un ou plusieurs cryptogrammes interdits imprimés sur la carte, et connus de la banque, et indiqués au propriétaire lors du courrier joint à l'envoi de la carte au propriétaire par sa banque. Ce ou ces cryptogrammes interdits, ont pour but de renforcer la sécurisation des transactions, en cas de vol de la carte. Si la carte était volée,

le voleur ne connaissant pas ces cryptogrammes interdits, pourrait en utiliser un, et être repéré par la banque.

10

REVENDICATIONS

1) Procédé de sécurisation des transactions par carte bancaire, associée à un compte bancaire, en ligne par téléphone ou fax, ou tout autre moyen nécessitant la divulgation des données sécuritaires, comportant le numéro de la carte bancaire, le nom et le prénom du propriétaire, la date d'expiration de la carte, caractérisé en ce qu'il comporte plusieurs cryptogrammes différents qui sont inscrits sur la carte bancaire, et reconnus par la banque, et en ce qu'après une transaction utilisant un de ces cryptogrammes, divulgué par le propriétaire pour effectuer sa transaction, la banque n'accepte plus l'utilisation de ce même cryptogramme pour la transaction suivante, ce même cryptogramme ne pouvant être accepté par la banque qu'après que le propriétaire ait effectué au moins une autre transaction utilisant au moins un autre cryptogramme inscrit sur la carte.

2) Procédé de sécurisation des transactions par carte bancaire, en ligne par téléphone ou fax ou tout autre moyen nécessitant la divulgation des données sécuritaires, selon la revendication 1, caractérisé en ce que plusieurs transactions dont le nombre est défini par la banque, avec des cryptogrammes différents, sont nécessaire pour pouvoir réutiliser le même cryptogramme.

3) Procédé de sécurisation des transactions par carte bancaire, en ligne par téléphone ou fax, ou tout autre moyen nécessitant la divulgation des données sécuritaires, selon la revendication 1,

caractérisé en ce que l'utilisation des cryptogrammes se fait dans un ordre prédéfini par la banque.

4) Procédé de sécurisation des transactions par carte bancaire, en ligne par téléphone ou fax, ou tout autre moyen nécessitant la divulgation des données sécuritaires, selon la revendication 1, caractérisé en ce que un ou plusieurs des cryptogrammes inscrits sur la carte sont interdits à l'utilisation, ces cryptogrammes sont choisis par la banque qui en informe le propriétaire de la carte.

5) Procédé de sécurisation des transactions par carte bancaire, en ligne par téléphone ou fax, ou tout autre moyen nécessitant la divulgation des données sécuritaires, selon les revendications 3 et 4, caractérisé en ce que les modes 3 et quatre selon l'invention peuvent être utilisés séparément ou en combinaison entre eux.

6) Procédé de sécurisation des transactions par carte bancaire, en ligne par téléphone ou fax, ou tout autre moyen nécessitant la divulgation des données sécuritaires, selon les revendications 1 à 5 caractérisé en ce que la banque contacte par téléphone ou SMS le propriétaire de la carte bancaire pour s'assurer qu'il n'a pas commis d'erreur en cas d'utilisation du même cryptogramme pour deux transactions successives, et si le propriétaire de la carte confirme qu'il n'a pas commis cette erreur, la banque conclut qu'elle est en présence d'une tentative de fraude, ce qui lui permet de lancer des investigations pour rechercher l'auteur de la tentative de fraude.

7) Procédé de sécurisation des transactions par carte bancaire, en ligne par téléphone ou fax, ou tout autre moyen nécessitant la divulgation des données sécuritaires, selon la revendication 4 caractérisé en ce que la banque contacte par téléphone ou SMS le propriétaire de la carte bancaire pour s'assurer qu'il n'a pas commis d'erreur en cas d'utilisation d'un des cryptogrammes interdits, et si le propriétaire de la carte confirme qu'il n'a pas commis cette erreur, la banque conclut qu'elle est en présence d'une tentative de fraude, ce qui lui permet de lancer des investigations pour rechercher l'auteur de la tentative de fraude.

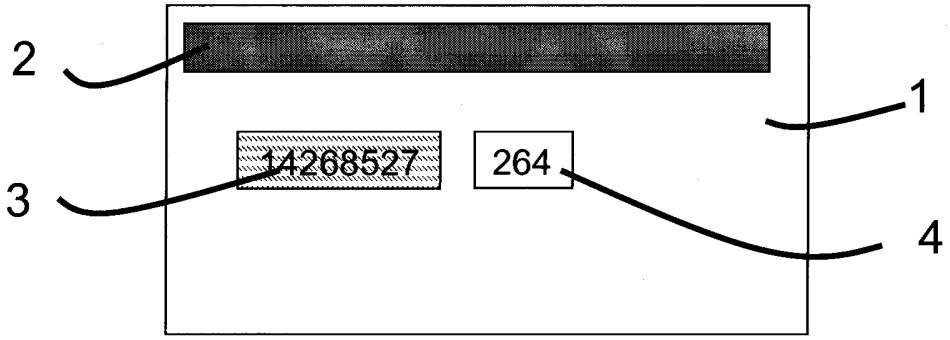


Fig 1

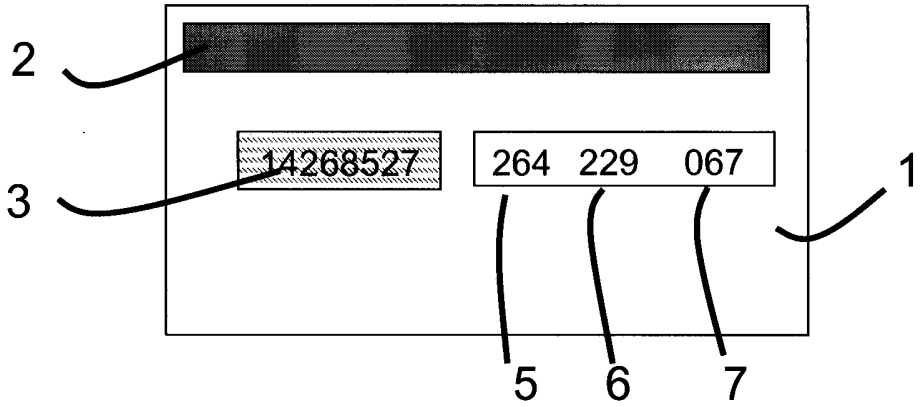


Fig 2

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 818808
FR 1502412

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		
Y	US 2007/250920 A1 (LINDSAY JEFFREY DEAN [US]) 25 octobre 2007 (2007-10-25)	1,4-7	H04L9/32 G06K19/077
A	* alinéa [0019] - alinéa [0034] * * alinéa [0120] - alinéa [0132] * * alinéa [0196] - alinéa [0201] * * alinéa [0260] - alinéa [0268] * * alinéa [0320] - alinéa [0325] * * figures 1,5,6 * * alinéa [0059] - alinéa [0060] *	2,3	

Y	US 2009/173782 A1 (MUSCATO MICHAEL A [US]) 9 juillet 2009 (2009-07-09)	1,4-7	
A	* alinéa [0009] - alinéa [0011] * * alinéa [0030] - alinéa [0035] * * alinéa [0041] - alinéa [0048] * * alinéa [0059] - alinéa [0067] * * figures 4,5,7 *	2,3	

A	US 7 427 033 B1 (ROSKIND JAMES [US]) 23 septembre 2008 (2008-09-23) * colonne 1, ligne 62 - colonne 4, ligne 45 * * colonne 5, ligne 9 - colonne 10, ligne 25 * * figures 3,7A,7B *	1-7	

			DOMAINES TECHNIQUES RECHERCHÉS (IPC) G06Q

Date d'achèvement de la recherche	Examinateur
7 juillet 2016	Sauzon, Guillaume

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

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1502412 FA 818808

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 07-07-2016
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 2007250920 A1	25-10-2007	US 2007250920 A1	25-10-2007
		US 2009259588 A1	15-10-2009
US 2009173782 A1	09-07-2009	EP 2245583 A1	03-11-2010
		US 2009173782 A1	09-07-2009
		US 2012059762 A1	08-03-2012
		US 2013054466 A1	28-02-2013
		WO 2009089099 A1	16-07-2009
US 7427033 B1	23-09-2008	US 7427033 B1	23-09-2008
		US 8820637 B1	02-09-2014
		US 2008308629 A1	18-12-2008
		US 2015026063 A1	22-01-2015
		US 2016125406 A1	05-05-2016

EPO FORM P0465