(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
5 juillet 2012 (05.07.2012)

WIPO | PCT

(10) Numéro de publication internationale
WO 2012/089953 A1

(51) Classification internationale des brevets : *G07F 7/10* (2006.01)

(21) Numéro de la demande internationale : PCT/FR2011/052922

(22) Date de dépôt international : 9 décembre 2011 (09.12.2011)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1061292 28 décembre 2010 (28.12.2010) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **PAYMIUM** [FR/FR]; 73 rue du Château, F-92100 Boulogne Billancourt (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : **GRANDVAL, Gonzague** [FR/FR]; 15 rue Bartholdi, F-92100 Boulogne Billancourt (FR).

(74) Mandataire : **PONTET ALLANO & ASSOCIES SELARL**; 6 avenue du Général de Gaulle, F-78000 Versailles (FR).

(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, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, 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 :

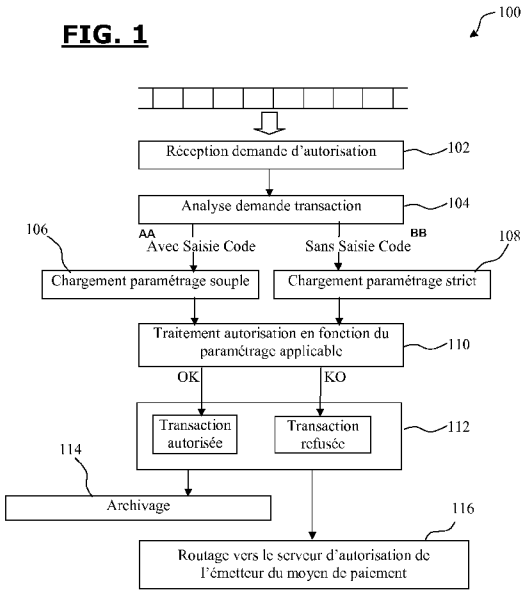
— *relative au droit du déposant de demander et d'obtenir un brevet (règle 4.17.ii))*

[Suite sur la page suivante]

(54) Title : METHOD OF PROCESSING DATA FOR THE MANAGEMENT OF TRANSACTIONS

(54) Titre : PROCEDE DE TRAITEMENT DE DONNEES POUR LA GESTION DE TRANSACTIONS

FIG. 1



102 Receive authorization request
104 Analyze transaction request
AA With code input
BB Without code input
106 Load flexible parameter setting
108 Load strict parameter setting
110 Process authorization as a function of the parameter setting applicable
112 Transaction authorized
Transaction refused
114 Archiving
116 Routing to the authorization server of the issuer of the payment means

(57) Abstract : The invention relates to a method for managing transactions generated by a means of payment forming the subject of a security code check and/or of a non-reusable authentication token and for which an authorization request may take place, characterized in that it comprises the following steps: analysis of the data associated with an authorization request so as to determine whether the said authorization request is generated with or without input of security code and/or non-reusable authentication token, making secure the said transaction by application, to said authorisation request, of security parameter settings (204, 206) which differ depending on whether said authorization request is generated with or without input of security code and/or non-reusable authentication token. It also relates to a system (200) implementing this method.

(57) Abrégé : L'invention concerne un procédé de gestion de transactions générées par un moyen de paiement faisant l'objet d'un contrôle de code de sécurité et/ou d'un jeton d'authentification non-rejouable, et pour lequel une demande d'autorisation peut avoir lieu, caractérisé en ce qu'il comprend les étapes suivantes : analyse des données associées à une demande d'autorisation pour déterminer si ladite demande d'autorisation est générée avec ou sans saisie de code de sécurité et/ou jeton d'authentification non-rejouable, sécurisation de ladite transaction par application, à ladite demande d'autorisation, de paramétrages de sécurisation (204,206) différents selon que ladite demande d'autorisation est générée avec ou sans saisie de code de sécurité et/ou jeton d'authentification non-rejouable. Elle concerne également un système (200) mettant en œuvre ce procédé.

WO 2012/089953 A1

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

— *relative à la qualité d'inventeur (règle 4.17.iv))*

Publiée :

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

« Procédé de traitement de données pour la gestion de transactions »

La présente invention concerne un procédé de traitement de données numériques pour la gestion de transactions. Elle concerne également un système mettant en œuvre un tel procédé.

Le domaine de l'invention est le domaine informatique, et plus particulièrement le domaine informatique appliqué à la gestion de transactions commerciales ou bancaires, réalisées à l'aide d'un moyen de paiement auquel est associé un code de sécurité, tels qu'une carte bancaire, une carte privative, une carte à puce, une carte à piste, une carte sans contact, un téléphone NFC avec application de paiement, ou encore un moyen de paiement virtuel telle qu'un e-wallet.

Actuellement, il existe des procédés de gestion de transactions avec un moyen de paiement en vue de s'assurer que les transactions réalisées correspondent bien aux transactions réellement demandées ou initiées par le porteur du moyen de paiement. Ces procédés ont pour but général d'éviter que le moyen de paiement, ou une réplique du moyen de paiement, soit utilisé par une personne autre que le porteur du moyen de paiement, éventuellement par une personne mal intentionnée, pour initier des transactions sans que le porteur du moyen de paiement soit au courant. Ces procédés consistent principalement en des procédures d'authentification du porteur auprès de l'émetteur du moyen de paiement.

Parmi les procédés et systèmes de gestion de transactions existants, certains prévoient un envoi d'information sur un appareil du porteur du moyen de paiement, par exemple un téléphone portable, après qu'une transaction est générée. Ces procédés et systèmes informant le porteur de la carte après la transaction, ne permettent pas d'empêcher la transaction.

D'autres procédés et système connus prévoient que le moyen de paiement soit constamment désactivé. Ainsi, lorsque le porteur du moyen de paiement désire réaliser une transaction, il active le moyen de paiement et réalise la transaction. Après la transaction le moyen de paiement est

désactivé, soit automatiquement, soit par le porteur du moyen de paiement. Un tel procédé permet effectivement d'éviter l'utilisation du moyen de paiement par une personne autre que le porteur du moyen de paiement.

Enfin, certains procédés et systèmes de gestion de transaction permettent de demander une confirmation au porteur du moyen de paiement grâce à un message envoyé par exemple sur un téléphone portable du porteur du moyen de paiement. Ces procédés et systèmes permettent d'éviter des fraudes mais restent lourds, parfois impossibles à mettre en place de façon efficace pour l'émetteur du moyen de paiement et à utiliser pour le porteur du moyen de paiement. En effet, la gestion des délais sur un réseau d'autorisation bancaire empêche l'exploitation de cette solution, qui elle-même devrait savoir distinguer les typologies de transactions. En outre, les transactions passent toujours en échec si le porteur ne peut être joint ou si l'acheminement du message à ce dernier prend trop de temps.

Un but de la présente invention est de remédier aux inconvénients précités.

Un autre but de la présente invention est de proposer un procédé et un système de gestion de transactions moins lourds à mettre en œuvre tout en étant au moins aussi efficaces que les procédés et systèmes actuels.

Un autre but de l'invention est de proposer un procédé et un système de gestion de transactions permettant de réaliser une gestion plus adaptée aux transactions réalisées avec un moyen de paiement.

Enfin, un autre but de la présente invention est de proposer un procédé et un système de gestion de transactions plus simple à gérer pour le porteur d'un moyen de paiement.

L'invention propose d'atteindre les buts précités par un procédé de gestion de transactions générées par un moyen de paiement faisant l'objet d'un contrôle de code de sécurité ou d'un jeton d'authentification non-rejouable, et pour lesquelles une demande d'autorisation peut avoir lieu. Le procédé selon l'invention comprend les étapes suivantes :

- analyse des données associées à une demande d'autorisation pour déterminer si ladite demande d'autorisation est générée avec ou sans

saisie de code de sécurité et/ou jeton d'authentification non-rejouable, et

- sécurisation de ladite transaction par application, à ladite demande d'autorisation, de paramétrages de sécurisation différents selon que ladite demande d'autorisation est générée avec ou sans saisie de code de sécurité ou jeton d'authentification non-rejouable.

Par moyen de paiement on entend, tout moyen de paiement auquel un code de sécurité, par exemple un code confidentiel, est attaché ou peut être attaché, tel que les cartes bancaires physiques ou virtuelles, des cartes de paiement privatives, des cartes de paiement à puce et/ou à piste, des e-wallets, des cartes sans contact et téléphones NFC.

Par « jeton d'authentification non-rejouable » on entend une donnée utilisée lors d'un processus d'authentification forte, par exemple de type 3D Secure, visant à demander au porteur du moyen de paiement de confirmer qu'il est bien en train de réaliser son paiement, en lui demandant de saisir une information que lui seul peut connaître. Il s'agit souvent d'un code unique envoyé par SMS ou tout autre dispositif (matrice de code, question personnelle, etc).Lorsque cette authentification non-rejouable du porteur a eu lieu, la demande d'autorisation est enrichie d'un jeton unique qui vient confirmer le bon déroulement de ce processus.

Dans la suite de la description, le mot « jeton » désignera« jeton d'authentification non-rejouable ».

Le procédé selon l'invention permet de réaliser une discrimination des transactions selon que la transaction a été initiée avec ou sans code de sécurité et/ou jeton, et d'appliquer un paramétrage de sécurisation aux transactions initiées avec saisie de code de sécurité et/ou jeton différent d'un paramétrage de sécurisation appliqué aux transactions initiées sans saisie de code de sécurité et/ou jeton.

Ainsi, le procédé selon l'invention permet d'appliquer un premier paramétrage de sécurisation lorsque la transaction est générée sans saisie de code de sécurité et/ou jeton, et un deuxième paramétrage de sécurisation lorsque la transaction est générée avec saisie de code de sécurité et/ou jeton.

Il est ainsi possible avec le procédé selon l'invention de prévoir un paramétrage de sécurisation qui est par exemple plus strict pour les transactions initiées sans saisie de code de sécurité et/ou jeton comparé au paramétrage de sécurisation pour les transactions initiées avec saisie de code de sécurité et/ou jeton.

Ainsi, le procédé selon l'invention permet de réaliser un traitement différent des demandes d'autorisation selon que le code de sécurité à été saisi ou non lors de la génération de la transaction et/ou selon que la transaction est réalisée avec ou sans jeton et d'adapter le degré de sécurisation en fonction. Le procédé selon l'invention est donc moins lourd à mettre en œuvre que les procédés de l'état de la technique qui prévoient d'appliquer le même paramétrage de sécurisation à toutes les demandes d'autorisation, tout en procurant une sécurisation au moins aussi efficace.

Par ailleurs, la gestion de transactions grâce au procédé selon l'invention est plus simple pour le porteur d'un moyen de paiement car il peut décider un paramétrage ne nécessitant pas d'intervention de sa part pour toutes les transactions réalisées avec saisie de code de sécurité par exemple. Ce qui lui permet de ne pas avoir à activer le moyen de paiement ou de confirmer la transaction pour toutes les transactions qu'il réalise avec saisie de code de sécurité.

En outre, le procédé de gestion de transactions selon l'invention permet de réaliser une gestion plus adaptée aux transactions puisqu'elle permet d'appliquer différents paramétrages de sécurisation en fonction du type de chacune des transactions.

Lorsque les données de demande d'autorisation se présentent sous la forme d'une trame comportant plusieurs champs, l'étape d'analyse des données de demande d'autorisation peut comprendre une analyse des données pertinentes de la demande d'autorisation pour déterminer s'il y a eu saisie du code de sécurité et/ou si les données comprennent un jeton. Les données pertinentes, peuvent comprendre un champ de la trame indiquant :

- une saisie ou non du code de sécurité,
- une présence ou non d'un jeton,

- s'il était demandé au porteur de saisir le code de sécurité. En effet, dans certains lieux de transactions, tels que par exemple les péages d'autoroutes, les transactions sont automatiquement réalisées sans demande de saisie de code de sécurité,
- un champ renseignant le pays dans lequel la transaction est réalisée, et/ou
- un certificat.

Avantageusement, le paramétrage de sécurisation appliquée à une demande d'autorisation sans saisie de code de sécurité et/ou jeton peut comprendre une émission d'une requête de confirmation de ladite autorisation vers un appareil de télécommunications au travers d'un réseau de communications. Ainsi, pour toutes les opérations réalisées sans saisie de code de sécurité ou jeton, une confirmation que la transaction est réalisée par le porteur légitime sera demandée avant la transaction. Si l'autorisation est refusée la transaction sera annulée. La transaction ne pourra être finalisée que si l'autorisation est accordée.

L'appareil de télécommunications peut être un téléphone portable, un Smartphone, une tablette Internet, un ordinateur ou tout autre appareil avec lequel il est possible de communiquer au travers d'un réseau de communication, tel le réseau Internet ou le réseau de téléphonie mobile.

Lorsque les données de demande d'autorisation se présentent sous la forme d'une trame comportant plusieurs champs, le paramétrage de sécurisation appliqué à une demande d'autorisation sans saisie de code de sécurité et/ou jeton peut comprendre un blocage/refus de ladite autorisation lorsque ladite trame comporte, pour au moins un champ préalablement spécifié, une valeur différente d'au moins une valeur préalablement spécifiée pour ledit champ.

Par exemple, le paramétrage de sécurisation peut comprendre une liste de pays autorisés. Lorsque la transaction a été initiée sans saisie de code de sécurité et/ou jeton dans un pays qui n'est pas spécifié pas dans la liste des pays autorisés, alors la demande d'autorisation est directement refusée. Dans ce cas, le procédé selon l'invention peut comprendre une

consultation du champ préalablement spécifié dans la trame, par exemple le champ « pays », et une comparaison de la valeur de ce champ avec une ou plusieurs valeurs prédéterminées pour ce champ.

La ou les valeurs préalablement renseignées pour le champ préalablement spécifié peuvent être des valeurs autorisées ou des valeurs interdites.

Le ou les champs spécifiés peuvent être relatifs, au pays de la transaction, au montant, à un des acteurs de la transaction, au circuit de la transaction, à la date, l'heure, la devise, etc.

Selon une particularité avantageuse du procédé selon l'invention, le paramétrage de sécurisation appliqué à une demande d'autorisation avec saisie de code de sécurité et/ou jeton peut comprendre une émission d'une requête de confirmation de ladite autorisation vers un appareil de télécommunications au travers d'un réseau de communications, si le montant de la transaction est supérieur à une valeur préalablement déterminée.

Cette caractéristique est particulièrement avantageuse, lorsque le porteur de la carte est une personne qui n'est pas majeure, par exemple un adolescent, et dont les transactions commerciales sont surveillées par son tuteur, par exemple un de ses parents. Ainsi, il est possible pour une deuxième personne de surveiller les dépenses réalisées par le porteur du moyen de paiement.

Par ailleurs, le paramétrage de sécurisation appliqué à une demande d'autorisation sans saisie de code de sécurité et/ou jeton, et/ou le paramétrage de sécurisation appliqué à une demande d'autorisation avec saisie de code de sécurité et/ou jeton peut être modifiable à distance au travers d'un réseau de communication, tel qu'un réseau de téléphonie ou le réseau Internet.

Le procédé selon l'invention peut en outre comprendre une désactivation/activation à distance d'un paramétrage de sécurisation, par exemple pour un période donnée limitée ou non.

De telles modifications, activations ou désactivations peuvent être réalisées avec une application mobile, un serveur vocal, par message courts dits « sms », sur un site internet sécurisé, etc.

Avantageusement, la modification, l'activation et/ou la désactivation à distance d'un paramétrage de sécurisation, ou d'un paramètre en particulier, peut être réalisée au moyen d'une connexion sécurisée.

Le procédé selon l'invention peut en outre comprendre un archivage d'au moins une modification réalisée par un porteur du moyen de paiement sur au moins un paramétrage de sécurisation afin d'assurer la traçabilité de toutes les actions et la gestion du risque.

Le procédé peut en outre comprendre la notification à l'utilisateur que sa demande de modification a bien été prise en compte.

En outre, le procédé selon l'invention peut également comprendre une génération d'un journal d'autorisations relatives au moyen de paiement concerné. Un tel journal peut comprendre une catégorisation des demandes d'autorisation dans des catégories telles que « transaction autorisée », « transaction refusée/bloquée », etc. et peut être mis à jour instantanément.

Le procédé selon l'invention peut être mis en œuvre pour la gestion de transactions de proximité, par exemple dans une situation de paiement en face à face c'est-à-dire avec présence du porteur sur le lieu de vente, dans une situation de retrait sur un DAB, un GAB ou un DAC (Distributeur Automatique de Billets, Guichet Automatique Bancaire, Distributeur Automatique de Carburant), et/ou pour la gestion de transactions réalisées à distance au travers d'un réseau de communication, par exemple les transactions réalisées par Internet ou par téléphone.

Dans un mode de réalisation particulier, le procédé selon l'invention peut être mis en œuvre en aval, en amont d'un serveur d'autorisation ou

intégré à un serveur d'autorisation d'un établissement émetteur du moyen de paiement.

Selon un autre aspect de l'invention il est proposé un programme informatique comprenant des instructions exécutables sur un appareil informatique pour mettre en œuvre les étapes du procédé selon l'invention.

Selon encore un autre aspect de l'invention il est proposé un système de gestion de transactions générées par un moyen de paiement faisant l'objet d'un contrôle de code de sécurité et/ou d'un jeton d'authentification non-rejouable et pour lesquelles une demande d'autorisation peut avoir lieu. Le système selon l'invention est caractérisé en ce qu'il comprend :

- des moyens d'analyse de données associées à une demande d'autorisation pour déterminer si ladite demande d'autorisation est générée avec ou sans saisie de code de sécurité et/ou jeton d'authentification non-rejouable, et
- des moyens de sécurisation de ladite transaction programmés pour appliquer à ladite demande d'autorisation des paramétrages de sécurisation différents selon que ladite demande d'autorisation est générée avec ou sans saisie de code de sécurité et/ou jeton d'authentification non-rejouable.

Le système selon l'invention peut comprendre un module d'émission d'une requête de confirmation de l'autorisation à un appareil de télécommunication distant.

Le système selon l'invention peut en outre comprendre une interface utilisateur agencée pour modifier, activer ou désactiver à distance un paramétrage de sécurisation au moyen d'une connexion sécurisée.

D'autres avantages et caractéristiques apparaîtront à l'examen de la description détaillée d'un mode de réalisation nullement limitatif, et des dessins annexés sur lesquels :

- la figure 1 est une représentation sous la forme d'un diagramme d'un procédé selon l'invention,
- la figure 2 est une représentation schématique d'un système selon l'invention, et
- les figures 3-5 sont plusieurs configurations dans lesquels le procédé et le système selon l'invention peuvent être mis en œuvre.

Sur les figures et dans la suite de la description, les éléments communs à plusieurs figures conservent la même référence.

Les exemples suivants concernent le traitement des transactions réalisées à l'aide d'un moyen de paiement auquel est associé un code de sécurité.

Dans les exemples suivants, les données associées à une demande d'autorisation sont analysées pour déterminer si ladite demande d'autorisation est générée avec ou sans saisie de code de sécurité uniquement.

Cependant, ces exemples peuvent être transposés au cas où les données associées à la demande d'autorisation sont analysées pour déterminer si ladite demande d'autorisation est générée avec ou sans jeton d'authentification non-rejouable en combinaison ou non avec la saisie ou non d'un code de sécurité.

La figure 1 est une représentation schématique des étapes d'un exemple d'un procédé 100 selon l'invention sous la forme d'un diagramme.

Le procédé 100 comprend une première étape 102 de réception d'une demande d'autorisation d'une transaction réalisée avec un moyen de paiement auquel un code de sécurité est associé (mais pas forcément utilisé pour la transaction). La demande d'autorisation comprend une trame (non représentée) de plusieurs champs de données, et notamment un ou plusieurs champs renseignant sur la saisie ou non d'un code de sécurité associé au moyen de paiement.

A l'étape 104, la trame de données est analysée pour déterminer si la transaction pour laquelle la demande d'autorisation a été générée avec ou

sans saisie de code. Le type de la transaction est donc déterminé à cette étape, à savoir : « avec saisie de code de sécurité » ou « sans saisie de code de sécurité ».

Si la transaction est réalisée avec saisie de code de sécurité c'est le paramétrage sécurisation, dit paramétrage souple, appliqué à ce type de transaction qui est chargé lors d'une étape 106.

Si la transaction est réalisée sans de code de sécurité c'est le paramétrage de sécurisation, dit paramétrage strict, appliqué à ce type de transaction qui est chargé lors d'une étape 108.

En fonction du paramétrage de sécurisation une étape 110 de traitement de la demande d'autorisation est réalisée pour déterminer une donnée d'autorisation, à savoir une donnée d'autorisation accordée, telle que « OK » ou une donnée d'autorisation refusée telle que « KO ». Le traitement peut comprendre :

- une comparaison de la valeur d'un ou plusieurs champs de la trame de la demande d'autorisation, préalablement spécifiés dans le paramétrage de sécurisation, à une ou plusieurs conditions associées à ces champs,
- émission d'une ou plusieurs requêtes de confirmation vers un appareil distant préalablement spécifié dans le paramétrage de sécurisation, et attente de la réponse à cette ou ces requêtes,
- etc.

En fonction des données d'autorisation déterminées lors de l'étape de traitement, la demande d'autorisation est soit acceptée soit refusée, lors d'une étape 112, par exemple par l'envoi d'une donnée d'acceptation de type « OK » ou par l'envoi d'une donnée de refus de type « KO ».

Le procédé 100 peut en outre comprendre une étape 114 d'archivage, dans des moyens de mémorisation, des demandes de transactions en association avec les données d'autorisation ainsi que le moyen de paiement concerné par les transactions.

Des modifications des paramétrages de sécurisation peuvent également être archivées dans les moyens de mémorisation.

Enfin, le procédé 100 comprend une étape 116 de routage de la demande d'autorisation enrichie de la donnée d'acceptation vers le serveur

d'autorisation de l'émetteur du moyen de paiement, qui peut finalement accepter ou refuser la transaction en fonction d'autres critères tels qu'un plafond de paiement autorisé atteint, fond insuffisant sur le compte concerné, etc.

La figure 2 est une représentation schématique d'un exemple de réalisation d'un système 200 selon l'invention.

Le système 200 comprend une interface utilisateur 202 permettant à un porteur d'un moyen de paiement de configurer un paramétrage de sécurisation souple 204 utilisé pour la gestion de transactions initiées avec saisie d'un code de sécurité associé au moyen de paiement, et un paramétrage de sécurisation strict 206 pour la gestion de transactions initiées sans saisie du code de sécurité associé au moyen de paiement.

La configuration des paramétrages de sécurisations 204 et 206 peut être réalisée au travers d'un réseau de communication, par exemple le réseau Internet 208, grâce à une connexion sécurisée 210, par exemple de type SSL.

La configuration peut être réalisée grâce à une application mobile 212 installée sur un appareil mobile, tel qu'un Smartphone 214.

Le système 200 comprend en outre une interface bancaire ou avec les réseaux d'autorisation216 permettant de recevoir des demandes d'autorisation depuis un réseau bancaire (non représenté) et d'émettre des données d'autorisation vers le réseau bancaire/d'autorisation grâce à une connexion 218, par exemple de type VPN (de l'anglais Virtual Private Network ou en français Réseau Privé Virtuel).

Le système 200 comprend en outre un module d'analyse 220 permettant de réaliser une analyse d'une demande d'autorisation et plus précisément d'une trame TR de champs transmise avec la demande d'autorisation.

Le module d'analyse 220 permet de déterminer le type TY de la transaction pour laquelle une demande d'autorisation a été reçue, à savoir, une transaction avec ou sans saisie de code.

Le module d'analyse 220transfère le type TY de la transaction ainsi que la trame TR à un module de traitement 222.

Le module de traitement 222 charge ou consulte le paramétrage de sécurité associé au type TY de la transaction, à savoir soit le paramétrage souple 204 soit le paramétrage strict 206.

Si besoin le module de traitement 222 demandera à un module de communication 224 d'émettre une ou plusieurs requêtes de confirmation vers l'appareil mobile 214.

Le module de traitement 222 émet une donnée d'autorisation, accordant ou refusant la transaction. Cette donnée sera communiquée au réseau bancaire/d'autorisation au travers de l'interface de connexion 216.

Le système 200 comprend en outre des moyens de mémorisation 226 dans lesquels sont mémorisés la demande d'autorisation, la donnée d'autorisation ainsi que le moyen de paiement concerné par la transaction.

Les moyens de mémorisation 226 mémorisent également les modifications des paramétrages de sécurisation 204 et 206.

Les figures 3-5 sont plusieurs configurations dans lesquels le procédé et le système selon l'invention peuvent être mis en œuvre.

Dans les configurations représentées sur les figures 3 à 5, la transaction est initiée chez un marchand 302 et transmise à la banque de l'acquéreur 304 au travers d'une connexion sécurisée. La banque acquéreur 304 transmet une demande d'autorisation 306 vers la banque émettrice308du moyen de paiement au travers d'un réseau bancaire ou d'un réseau privatif 310. En réponse à la donnée d'autorisation, une donnée d'autorisation 312 par exemple « OK » ou « KO », est déterminée par le système 200 de la figure 2. Cette donnée d'autorisation 312 est ensuite transmise par la banque émettrice 308 à la banque acquéreur 304 au travers du réseau bancaire ou privatif 310.

Le procédé selon l'invention ne se substitue pas aux serveurs d'autorisation de l'émetteur. Ainsi, si le procédé indique qu'une transaction est OK, l'établissement émetteur peut tout à fait décider de refuser la demande d'autorisation sur d'autres critères (plafond de paiement atteint, etc.). Ainsi, le procédé selon l'invention marque les demandes d'autorisation de transaction pour qu'elles soient traitées ensuite chez l'émetteur en connaissance des paramètres surveillés par le procédé.

Dans la configuration 300 de la figure 3, le système 200 selon l'invention est situé à distance de la banque émettrice 308 et est connecté à la banque émettrice au travers d'une connexion 218 sécurisée de type VPN. La demande d'autorisation 306 est transmise au système 200 par la banque émettrice 308 et la donnée d'autorisation déterminée par le système 200 est transmise à la banque émettrice 308 qui l'envoie à la banque acquéreur 304. Autrement dit, le système 200 se trouve en dehors des infrastructures d'autorisations de l'organisme émetteur du moyen de paiement, avec lesquelles elle est cependant interfacée via un réseau sécurisée.

Dans la configuration 400 représentée sur la figure 4, le système 200 selon l'invention est situé dans la banque émettrice 308, c'est-à-dire au sein même des infrastructures d'autorisations de l'organisme émetteur du moyen de paiement.

Dans la configuration 500 représentée sur la figure 5, le système 200 selon l'invention est situé entre la banque acquéreur 304 et la banque émettrice308. Autrement dit, le système 200 selon l'invention se trouve au sein des infrastructures de transport du fournisseur de services de routage sécurisé et le procédé constitue un service à valeur ajouté pour l'établissement émetteur destinataire de la demande d'autorisation « enrichie » par le système 200.L'information complémentaire transmise par le procédé constitue une sorte de scoring supplémentaire venant s'ajouter aux autres éléments de décision du serveur d'autorisation de l'établissement émetteur.

Nous allons maintenant décrire un exemple de paramétrage strict, pour les transactions ayant été réalisées sans saisie du code personnel. Le paramétrage strict comprend :

- a) montant plafond à 100€, et
- b) devise autorisée : Euro, et
- c) confirmation nécessaire par le porteur.

Ainsi, une demande d'autorisation pour une transaction d'un montant supérieur à 100€ sera refusée, ou plus précisément sera enrichie d'une

information indiquant à l'établissement émetteur que le porteur refuse cette transaction. Il en serait de même pour une transaction de 10$, où le critère devise sera suffisant pour rejeter cette transaction.

Dans le cas où les conditions a) et b) sont respectées, et que le porteur, sollicité sur son mobile, ne répond pas alors la transaction sera rejetée.

Nous allons maintenant décrire un exemple de paramétrage souple, pour les transactions ayant été réalisées avec saisie du code personnel. Le paramétrage souple pourrait relever des mêmes règles a) et b) mais pas de la règle c). Dans ce cas, si les conditions a) et b) sont respectées, et que le porteur ne répond pas suite à une première sollicitation sur le mobile, le système indique que la transaction devra être traitée de façon standard par l'établissement émetteur.

Nous allons maintenant donner un exemple de trame d'une demande d'autorisation française respectant des normes ISO (8583) utilisées dans d'autres pays que la France.

X: Obligatoire

C: Conditionnel

F: Facultatif

.: Champ non traité

S: Valeur spécifique au message

Q: Valeur comme la question

QI: Valeur comme la question initiale

RI: Valeur comme la réponse initiale

A: Demande d'autorisation: 0100

B: Réponse à demande d'autorisation : 0110

N°	Définition	A	B
1	Présence deuxième bit map	C(1)	C(1)
2	Numéro de porteur	XS	XQ
3	Code de traitement	XS	XQ
4	Montant de la transaction	XS	XQ

7 Date et heure de transmission XS XS

11 Numéro d'audit XS XQ

12 Heure locale de la transaction XS FQ

13 Date locale de la transaction XS FQ

14 Date d'expiration XS FQ

15 Date de règlementC(6)

18 Code activité de l'accepteur XS FQ

22 Mode de lecture du système d'acceptation XS FQ

25 Conditions de la transaction au point de service XS FQ

27 Longueur du numéro d'autorisation C(7).

32 Identification de l'organisme acquéreur XS XQ

33 Identification de l'organisme transmetteur C(21) FQ

37 Numéro de référence d'archivage F FQ

38 Autorisation, réponse d'identificationC(10)

39 Code réponseXS

41 Identification du système d'acceptation XS XQ

42 Identification de l'accepteur de carte XS XQ

43 Nom et adresse de l'accepteur de carte FS FQ

44 Données complémentaires de réponseC(2)

AA Champ erronéC(69)

AB Erreur de sécuritéC(12)

AC Conversion de champFS

AF Code activation serviceFS

BB Numéro de téléphoneFS

BC Message à destination de l'initiateur de la transactionFS

CA Informations relatives au traitement du CVV/CVC C(12)

CB Informations relatives au contrôle du cryptogramme C(12)

47 Données complémentaires nationales C(2) C(2)

08 Type de site C(63) FQ

24 Numéro de dossier C(110) C(110)

95 Données de réseau C(6)

96 SIRET C(63) FQ

97 IDPA C(63) FQ

A0 IDSA C(63) FQ

49 Code monnaie de la transaction XS XQ

53 Informations liées à la sécurité XS XS

59 Données nationales C(2) C(2)

0100 Code fonction C(98) FQ

0101 Code raison du message XS FQ

0102 Année de la transaction XS CQ(95)

0200 Environnement règlementaire et technique de la transaction XS FQ

0201 ITP (Identifiant de l'application Terminal) XS FQ

0202 Numéro de contrat accepteur X FQ
0203 Numéro logique du système d'acceptation XS FQ
0204 Numéro logique du point d'acceptation C(22) FQ
0205 Code pays du système d'acceptation X
0207 Montant cumulé par porteur X FQ
020B Type d'applicatif du système d'acceptation (TASA) X FQ
0210 Référence client 1 C(109)
0211 Référence client 2 C(109)
0212 Numéro de marché C(109)
0213 Montant de TVA C(109)
0300 Cryptogramme visuel X
0301 Informations relatives au contrôle du cryptogramme visuel C(12)
0400 Identifiant transaction fourni par l'accepteur C(99)
0401 Cryptogramme commerce électronique C(99)
0407 Type de sécurisation de transaction de commerce électronique C(5)
0409 Informations relatives au traitement du cryptogramme commerce électronique C(12)
0410 Méthode d'authentification porteur utilisée par l'émetteur C(6)
0411 Méthode de calcul du cryptogramme de commerce électronique C(101)
0412 Résultat de l'utilisation de l'architecture de paiement sécurisé VADS C(102)
0413 Mode de sécurisation de la transaction modifiéC(6)
0800 Type de facture / procédure C(13) CQ(13).

Bien entendu, l'invention n'est pas limitée aux exemples qui viennent d'être décrits.

REVENDICATIONS

1. Procédé de gestion de transactions générées par un moyen de paiement faisant l'objet d'un contrôle de code de sécurité et/ou d'un jeton d'authentification non-rejouable et pour lesquelles une demande d'autorisation (306) peut avoir lieu, ledit procédé comprenant les étapes suivantes :

- analyse (104) des données associées à une demande d'autorisation (306) pour déterminer si ladite demande d'autorisation (306) est générée avec ou sans saisie de code de sécurité et/ou jeton d'authentification non-rejouable,
- sécurisation de ladite transaction par application (110), à ladite demande d'autorisation (306), de paramétrages de sécurisation (204, 206) différents selon que ladite demande d'autorisation (306) est générée avec ou sans saisie de code de sécurité et/ou jeton d'authentification non-rejouable ;

caractérisé en ce que :

- le paramétrage de sécurisation (206) appliqué à une demande d'autorisation (306) sans saisie de code de sécurité et/ou jeton d'authentification non-rejouable ;et/ou
- le paramétrage de sécurisation (204) appliqué à une demande d'autorisation (306) avec saisie de code de sécurité et/ou jeton d'authentification non-rejouable ;

est modifiable à distance au travers d'un réseau (208) de communication.

2. Procédé selon la revendication 1, caractérisé en ce que les données de demande d'autorisation se présentent sous la forme d'une trame comportant plusieurs champs, l'étape d'analyse (104) des données de demande d'autorisation (306) comprenant une analyse des données pertinentes de la demande d'autorisation pour déterminer s'il y a eu saisie du code de sécurité ou jeton d'authentification non-rejouable.

3. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que le paramétrage de sécurisation (206) appliquée à une

demande d'autorisation (306) sans saisie de code de sécurité et/ou jeton d'authentification non-rejouable comprend une émission d'une requête de confirmation de ladite autorisation vers un appareil (214) de télécommunications au travers d'un réseau (208) de communications.

4. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que les données de demande d'autorisation se présentent sous la forme d'une trame comportant plusieurs champs, et en ce que le paramétrage de sécurisation (204) appliqué à une demande d'autorisation (306) sans saisie de code de sécurité et/ou jeton d'authentification non-rejouable comprend un blocage/refus de ladite autorisation lorsque ladite trame comporte, pour au moins un champ préalablement spécifié, une valeur différente d'au moins une valeur préalablement spécifiée pour ledit champ.

5. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que le paramétrage de sécurisation (204) appliqué à une demande d'autorisation (306) avec saisie de code de sécurité et/ou jeton d'authentification non-rejouable comprend une émission d'une requête de confirmation de ladite autorisation vers un appareil (214) de télécommunications au travers d'un réseau (208) de communications, si le montant de la transaction est supérieur à une valeur préalablement déterminée.

6. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend en outre une désactivation/activation à distance d'un paramétrage de sécurisation (204, 206).

7. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend un archivage d'au moins une modification réalisée par un porteur du moyen de paiement sur au moins un paramétrage de sécurisation.

8. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend en outre une génération d'un journal d'autorisations relatives au moyen de paiement concerné.

9. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il est mis en œuvre pour la gestion de transactions de proximité, sur automates ou de transactions réalisées à distance au travers d'un réseau de communication.

10. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il est mis en œuvre en aval, en amont ou intégré à un serveur d'autorisation d'un établissement émetteur du moyen de paiement.

11. Programme informatique comprenant des instructions exécutables sur un appareil informatique pour mettre en œuvre les étapes du procédé selon l'une quelconque des revendications précédentes.

12. Système (200) de gestion de transactions générées par un moyen de paiement faisant l'objet d'un contrôle de code de sécurité et/ou d'un jeton d'authentification non-rejouable et pour lesquelles une demande d'autorisation (306) peut avoir lieu, ledit système comprenant :

- des moyens (220) d'analyse des données associées à une demande d'autorisation (306) pour déterminer si ladite demande d'autorisation est générée avec ou sans saisie de code de sécurité et/ou jeton d'authentification non-rejouable,
- des moyens (222, 224, 204, 206) de sécurisation de ladite transaction programmés pour appliquer à ladite demande d'autorisation (306) des paramétrages de sécurisation (204, 206) différents selon que ladite demande d'autorisation (306) est générée avec ou sans saisie de code de sécurité et/ou jeton d'authentification non-rejouable ;

caractérisé en ce que ledit système comprend en outre une interface (202) utilisateur agencée pour modifier, activer ou désactiver à distance un

paramétrage de sécurisation (204, 206) au moyen d'une connexion (210) sécurisée.

13. Système selon la revendication 12, caractérisé en ce qu'il comprend un module (224) d'émission d'une requête de confirmation de l'autorisation à un appareil (214) de télécommunication distant.

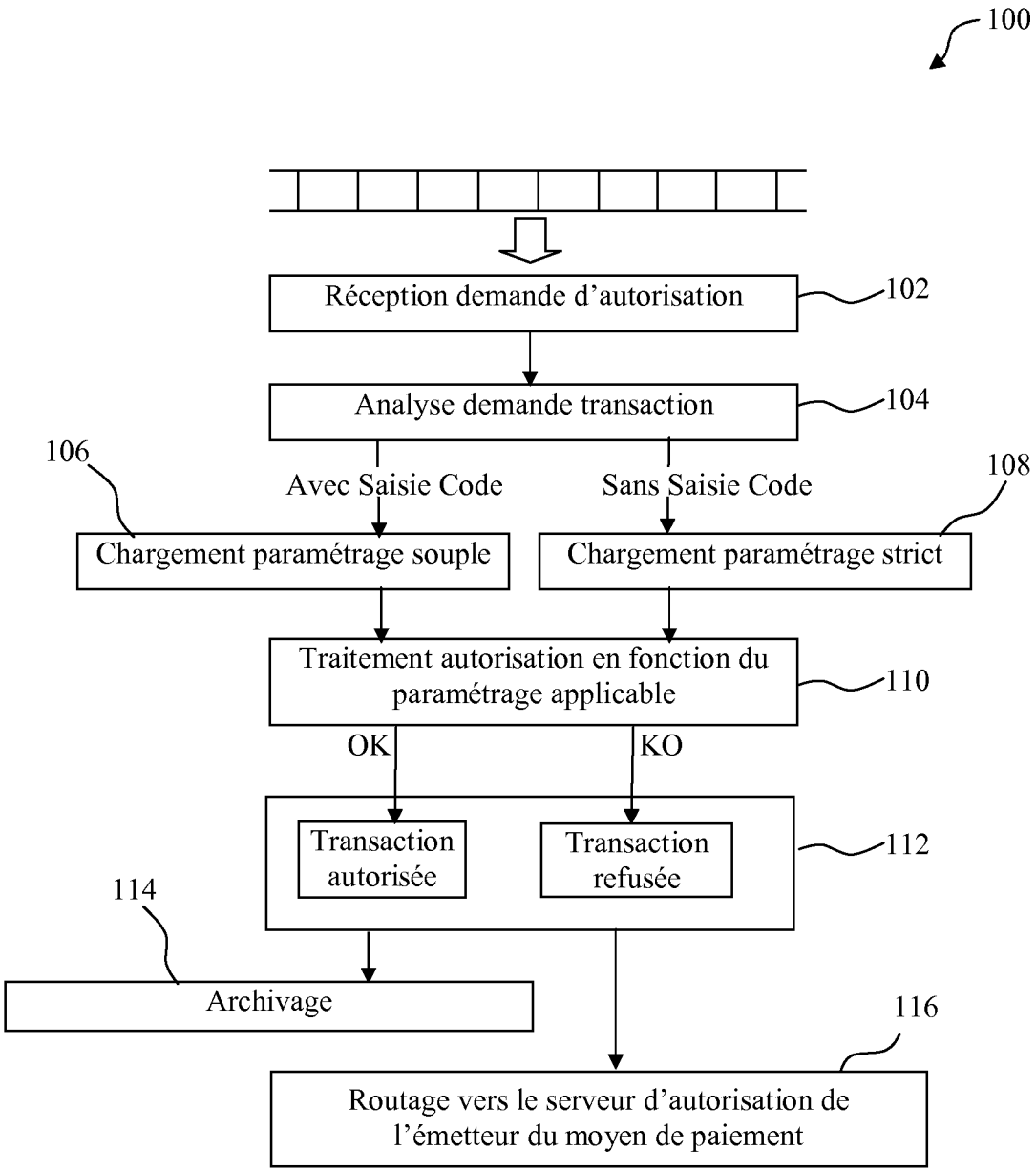

100
Réception demande d'autorisation
102
Analyse demande transaction
104
106
Avec Saisie Code
Sans Saisie Code
108
Chargement paramétrage souple
Chargement paramétrage strict
Traitement autorisation en fonction du paramétrage applicable
110
OK
KO
Transaction autorisée
Transaction refusée
112
114
Archivage
116
Routage vers le serveur d'autorisation de l'émetteur du moyen de paiement

FIG. 1

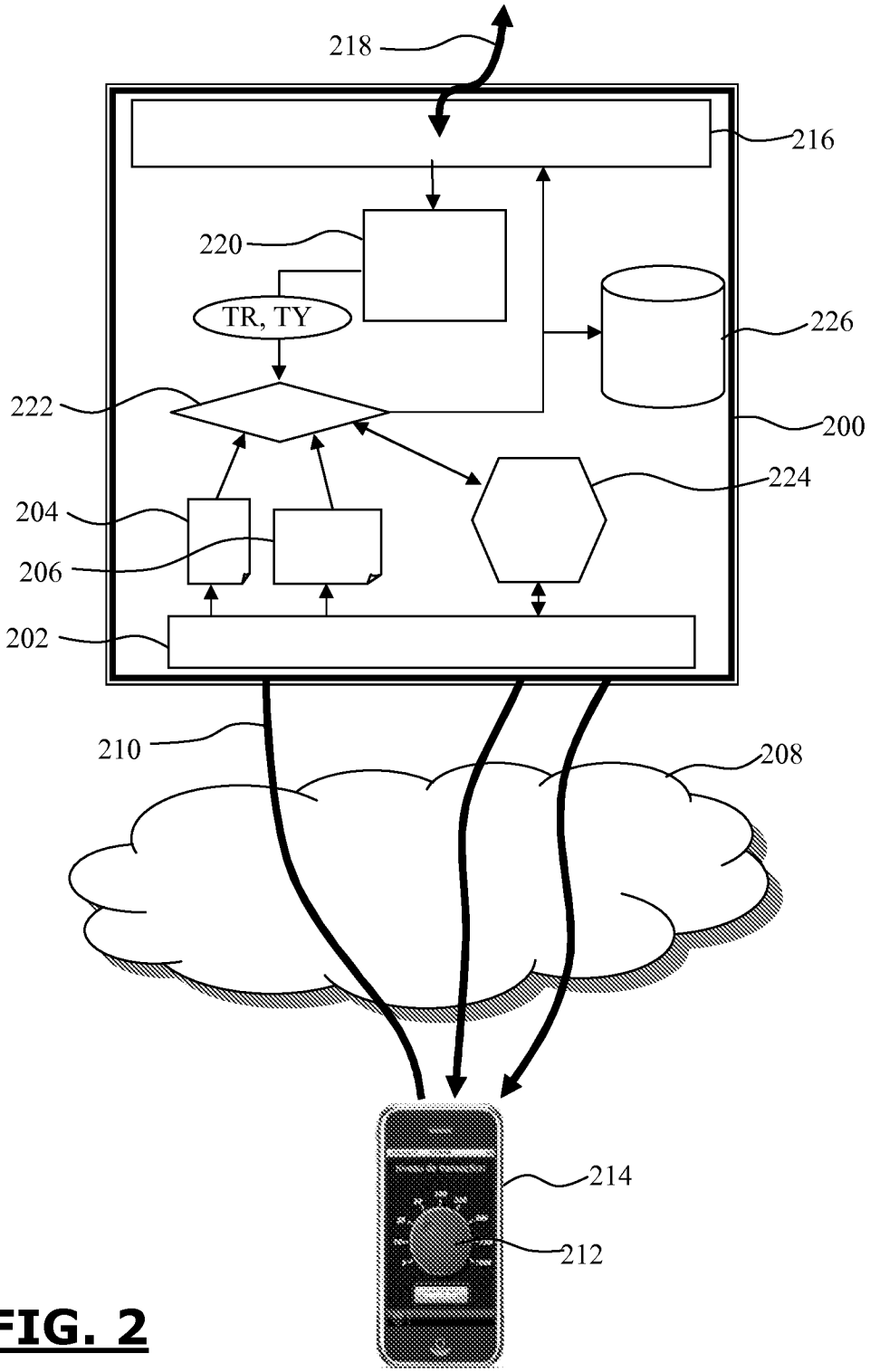


FIG. 2

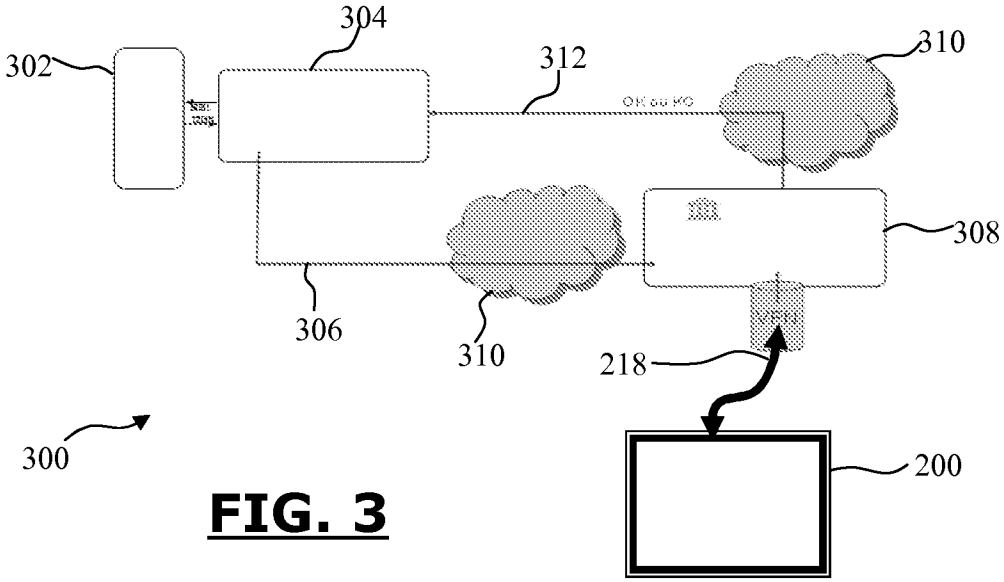

304
302
312
310
OK ou KO
308
306
310
218
300
200

FIG. 3

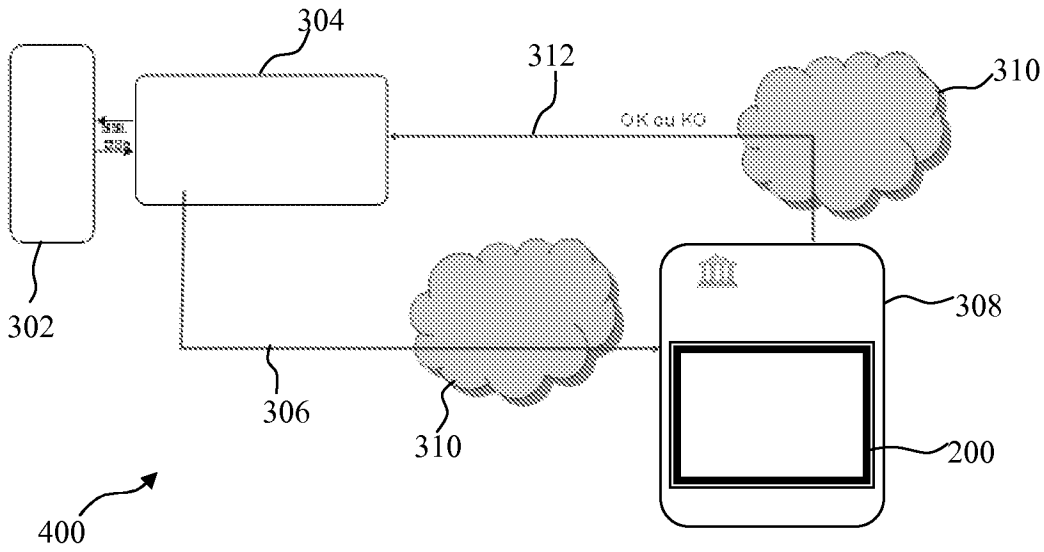

304
312
310
OK ou KO
302
308
306
310
200
400

FIG. 4

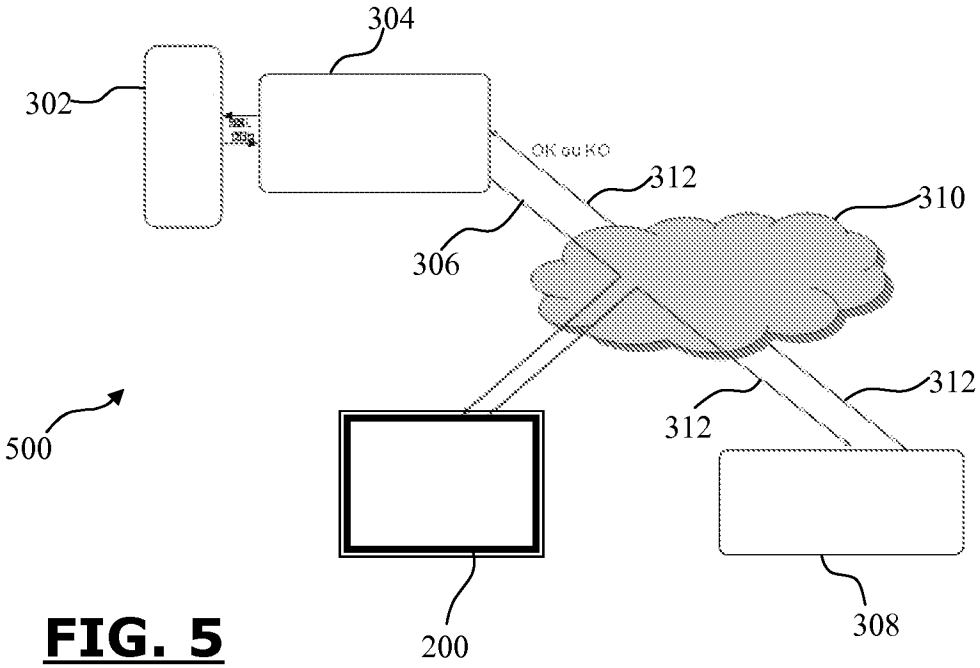


FIG. 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2011/052922

A. CLASSIFICATION OF SUBJECT MATTER
INV. G07F7/10
ADD.

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)
G07F

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	US 2003/144952 A1 (BROWN MICHAEL WAYNE [US] ET AL) 31 July 2003 (2003-07-31) paragraphs [0019] - [0021], [0024], [0025], [0028], [0031], [0032], [0034], [0037], [0044], [0045] figure 2	1-13
A	WO 2010/129317 A2 (VISA INT SERVICE ASS [US]; CARLSON MARK [US]; MAYOR SHALINI [US]) 11 November 2010 (2010-11-11) paragraphs [0021], [0023] - [0026], [0028] - [0031], [0034], [0035], [0037], [0040] - [0046], [0052], [0057], [0058] figures 1-4	1-13

☐ 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
10 February 2012	28/02/2012

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	Spitaler, Thomas

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2011/052922

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003144952 A1	31-07-2003	NONE	
WO 2010129317 A2	11-11-2010	US 2010325047 A1	23-12-2010
		WO 2010129317 A2	11-11-2010

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2011/052922

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G07F7/10
ADD.

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)
G07F

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	US 2003/144952 A1 (BROWN MICHAEL WAYNE [US] ET AL) 31 juillet 2003 (2003-07-31) alinéas [0019] - [0021], [0024], [0025], [0028], [0031], [0032], [0034], [0037], [0044], [0045] figure 2	1-13

A	WO 2010/129317 A2 (VISA INT SERVICE ASS [US]; CARLSON MARK [US]; MAYOR SHALINI [US]) 11 novembre 2010 (2010-11-11) alinéas [0021], [0023] - [0026], [0028] - [0031], [0034], [0035], [0037], [0040] - [0046], [0052], [0057], [0058] figures 1-4	1-13

☐ 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
10 février 2012	28/02/2012

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	Spitaler, Thomas

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2011/052922

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2003144952 A1	31-07-2003	AUCUN	
WO 2010129317 A2	11-11-2010	US 2010325047 A1	23-12-2010
		WO 2010129317 A2	11-11-2010