(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
13 février 2003 (13.02.2003)

PCT

(10) Numéro de publication internationale
WO 03/012703 A2

(51) Classification internationale des brevets[7] : G06F 17/60

(21) Numéro de la demande internationale :
PCT/FR02/02671

(22) Date de dépôt international : 25 juillet 2002 (25.07.2002)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
01/10138 27 juillet 2001 (27.07.2001) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **SMART DESIGN** [FR/FR]; 35, boulevard des Plants, F-78860 Saint Nom La Breteche (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(pour US seulement)* : **EONNET, Yves** [FR/FR]; 35, boulevard des Plants, F-78860 Saint Nom La Breteche (FR). **GUELTON, Evrard** [FR/FR]; 4, rue des Chartreux, F-75006 Paris (FR). **RIGAL, Vincent** [FR/FR]; 40, avenue de la Gare, F-92330 Sceaux (FR).

(74) Mandataire : **ERNEST GUTMANN - YVES PLASSERAUD S.A.**; 3, rue Chauveau-Lagarde, F-75008 Paris (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :
— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) **Title:** METHOD FOR MAKING TRANSACTIONS SECURE

(54) **Titre :** PROCEDE DE SECURISATION DE TRANSACTIONS

(57) **Abstract:** The invention concerns a method for making secure transactions carried out by means of media such as bank cards and the like, said method consisting in sending through a merchant an authorisation or payment request to a server, said request comprising data concerning the transaction and terms and conditions for reading data on the medium used, the method further consisting in: associating with each medium a means for communication with the bearer of the medium, using the data included in the authorisation or payment request to determine risky transactions and sending to the bearer a message indicating a risky transaction, after the bank has authorised the transaction.

(57) **Abrégé :** Procédé de sécurisation de transactions effectuées au moyen de supports tels que des cartes bancaires et analogues, ce procédé consistant à faire envoyer par un marchand une demande d'autorisation ou de paiement à un serveur, cette demande comportant des informations relatives à la transaction et aux modalités de lecture d'informations sur le support utilisé, le procédé consistant également : à associer à chaque support un moyen de communication avec le titulaire du support, à utiliser les informations incluses dans la demande d'autorisation ou de paiement pour determiner les transactions a risque, et à envoyer au titulaire un message lui signalant une transaction à risque, apres autorisation de la transaction par la banque.

WO 03/012703 A2

Procédé de sécurisation de transactions

L'invention concerne un procédé de sécurisation de transactions financières effectuées au moyen de supports tels que des cartes bancaires ou analogues.

Dans la technique actuelle, lorsqu'un marchand et un acheteur ont défini une transaction, par exemple en vente à distance ou via le réseau internet, cette transaction peut être décrite, en ce qui concerne son paiement, par une identification d'une carte de paiement (numéro de carte, appelé PAN, et date d'expiration), un montant, l'identité du marchand, voire l'identité de l'acheteur. Elle est également caractérisée par un ensemble d'informations sur les modalités techniques de la transaction, contenues dans des champs des messages informatiques qui transitent dans les réseaux financiers.

Généralement, le marchand envoie cette transaction à sa banque ou à une passerelle intermédiaire, comme un centre de télécollecte ou une passerelle de télépaiement, sous la forme d'une demande d'autorisation. Celle-ci est dirigée vers la banque de l'acheteur qui dispose de quelques secondes pour vérifier le statut de la carte et ses plafonds, avant d'autoriser ou de rejeter la transaction.

Le marchand expédie ensuite la marchandise et présente une demande de paiement. Celle-ci suit le même trajet que la demande d'autorisation, passant par une éventuelle passerelle, la banque du marchand, généralement les réseaux interbancaires et arrivant à la banque de l'acheteur.

La plupart des systèmes de transactions sécurisées demandent un double équipement, tant du

marchand que de l'acheteur, nécessaire pour sécuriser la transaction. Un exemple est celui du système de cartes à puce, généralisé en France en 1993, avec ses cartes et ses terminaux de paiement, qui utilisent un lecteur de cartes à puce sur le micro-ordinateur de l'acheteur en ligne, ainsi qu'une passerelle de paiement sécurisé du coté du marchand. Les systèmes utilisant des téléphones portables à double fente imposent la modification du téléphone de l'acheteur, ainsi qu'une passerelle de paiement spécifique coté marchand.

Cette contrainte de double équipement rend le déploiement de telles solutions extrêmement difficile. En effet, le marchand n'a intérêt à investir que si un nombre suffisant de ses clients sont équipés, et réciproquement. De plus, l'acheteur n'est en sécurité que quand tous les marchands sont équipés, faute de quoi un fraudeur tentera des paiements auprès des vendeurs non sécurisés.

Les documents EP-A-0745961 et FR-A-2 792 143 décrivent des systèmes de sécurisation qui ne présentent pas ces deux défauts, car ils ne nécessitent des moyens particuliers que du côté acheteur ou du côté client.

Ce procédé décrit par le document FR-A-2 792 143 comprend l'émission de demandes d'autorisation par les marchands. Quand une telle demande est reçue, le téléphone portable de l'acheteur est localisé, on compare les localisations du téléphone et du point de vente, et on demande confirmation à l'acheteur si les deux localisations sont différentes. Ce système peut être inopérant en vente à distance, alors que ce type de vente est particulièrement propice à la fraude, car il risque d'être trop lent pour permettre un

rejet de l'autorisation, et donc ne peut empêcher la transaction d'être conclue et la marchandise livrée, alors même que le titulaire de la carte est en train de prévenir le système qu'une fraude est en cours.

De plus, on ne peut légalement obtenir la localisation du téléphone portable qu'avec l'accord de son titulaire. Celui-ci ne le donnera que dans la mesure où il y voit un intérêt. Or les cas de fraudes détectables par le système, quoique financièrement très pénalisants, sont peu connus du grand public qui n'y est pas sensibilisé.

Le document EP-A-0745961 décrit un procédé qui ne fait intervenir de moyens particuliers que coté acheteur. Ce procédé comprend un mécanisme d'interception des demandes d'autorisation par la banque émettrice. A la réception de ces demandes, la banque envoie un message vers l'acheteur, typiquement par un moyen téléphonique. L'acheteur peut ainsi s'opposer à la transaction, conduisant la banque à envoyer un refus d'autorisation vers le marchand. Selon les modes de réalisation, ce refus est envoyé sur contestation par l'acheteur ou sur absence de réponse de sa part dans un délai donné.

Ce système est en fait inopérant. En effet, les réseaux monétique comporte un règle essentielle, qui impose aux serveurs d'autorisation un temps de réponse très bref (de quelques secondes). Il est en pratique impossible dans un tel laps de temps d'envoyer un message au client et d'obtenir sa réponse et le système décrit par le document EP-A-0745961 produirait donc un rejet systématique. Il ne pourrait fonctionner pratiquement que si cette règle était modifiée. Or une telle modification est très difficile à envisager, pour des raisons techniques

(elle est incluse dans l'ensemble des réseaux bancaires et dans l'ensemble des serveurs d'autorisation du monde) et pour des raisons fonctionnelles (cette règle est essentielle pour la fluidité du trafic monétique et pour la rapidité des passages des clients aux caisses).

On connaît également un système de sécurisation des transactions appelé carte virtuelle, dans lequel un numéro de carte particulier est délivré pour les transactions à distance. Ceci élimine le risque que ce numéro, obtenu par un fraudeur, soit utilisé pour d'autres transactions, car il n'est valable que pour une seule transaction avant d'être neutralisé.

Mais ce système présente lui aussi des limites sur le plan de la sécurité, car il n'empêche pas un fraudeur d'utiliser le numéro de carte réel pour des transactions à distance. On pourrait prévoir d'interdire systématiquement l'usage de ce numéro en vente à distance, mais cette solution apparaît très pénalisante tant pour les banques (elle apparaît comme une limitation au commerce) que pour les porteurs qui, en pratique, ne pourraient plus utiliser un paiement par carte sur les sites de vente à distance traditionnels, car la fourniture des numéros de carte virtuels n'est commode que sur un réseau du type internet.

Ce système de carte virtuelle comporte également un risque important d'erreur par le porteur, qui peut notamment oublier de demander un numéro virtuel et commander avec son numéro réel.

La présente invention a pour but d'apporter une solution simple et efficace à ces problèmes.

Elle propose à cet effet un procédé de

sécurisation de transactions effectuées entre des marchands et des acheteurs au moyen de supports d'informations tels que des cartes bancaires et analogues, ce procédé consistant à associer, dans une banque de données protégée, chaque support et un moyen de communication avec le titulaire du support, et à faire envoyer par un terminal marchand une demande d'autorisation ou de paiement à un serveur d'autorisation ou de paiement, cette demande comportant des informations relatives à la transaction et aux modalités de lecture d'informations sur le support utilisé par l'acheteur, caractérisé en ce qu'il consiste également :

- à utiliser lesdites informations incluses dans la demande d'autorisation de transaction ou de paiement pour déterminer si la transaction est à risque ou non,

- si oui, à envoyer au titulaire du support, par le moyen de communication, un message d'alerte lui signalant la transaction à risque, une fois l'autorisation accordée par le banque.

Avantageusement, ce procédé consiste également à demander au titulaire s'il est bien l'auteur de la transaction afin éventuellement de mettre la carte en opposition ou de stopper l'expédition de la marchandise.

On peut aussi proposer au titulaire de refuser la transaction et de demander à la banque de recréditer son compte du montant de la transaction.

L'invention ne comporte de moyens que du côté de

l'acheteur et de sa banque. On évite ainsi les inconvénients dus à la contrainte de double équipement. L'invention s'inscrit dans le cadre des règles monétiques existantes, dont elle ne suppose aucune modification. En particulier, elle ne suppose aucune intervention sur le fonctionnement des serveurs d'autorisation des banques : le système selon l'invention peut se contenter de recevoir, en léger différé, copie des autorisations accordées par la banque. Ce point est particulièrement important, car ces serveurs sont souvent des machines extrêmement complexes, résultats de dizaines de modifications successives, et dont le fonctionnement est critique : toute interruption se traduit par une impossibilité de paiement pour les clients de la banque. D'une manière générale, l'invention permet une mise en œuvre extrêmement rapide et peu coûteuse, pratiquement sans investissement matériel (ni pour la banque, ni pour l'acheteur, ni pour le marchand) et sans modification informatique au sein de la banque ou chez le marchand.

En contrepartie de ces avantages, l'invention ne permet pas à l'acheteur de bloquer la transaction au moment de la demande d'autorisation. En revanche, elle permet une mise en opposition très rapide, interdisant au fraudeur de réutiliser une carte. L'invention permet donc une limitation très importante de la fraude.

Selon une autre caractéristique de l'invention, deux mécanismes principaux d'identification des transactions à risque sont proposés et peuvent être utilisés séparément ou en combinaison.

Le premier mécanisme utilise les informations décrivant les conditions réglementaires de la

transaction.

Les messages monétiques contiennent un ensemble d'informations utilisables pour ce faire, mais dont aucune n'est suffisante. Le champ 25 des demandes d'autorisation (norme ISO 8583, « conditions de la transaction au point de service ») donne normalement l'information de vente à distance. En pratique, il n'est pas toujours renseigné de manière fiable, notamment en France. Il doit donc être complété par le champ 59 (données nationales) type 200 (environnement technique et réglementaire) pour les transactions françaises au moins. Si ce champ comporte une valeur entre 20 et 23, entre 30 et 33 ou vaut 35, il s'agit d'une vente à distance non sécurisée. S'il vaut 24 ou 34, on se reportera au champ 59 type 407, qui donne des indications sur le niveau de sécurité.

Dans le cas des messages venant des réseaux VISA, la procédure est analogue.

Dans le cas des messages venant des réseaux Europay/Mastercard, il convient également de considérer le champ 25, car le seul champ 59 n'est pas renseigné de manière fiable.

Ce procédé indique avec une bonne probabilité les transactions en vente à distance, et de manière fiable celles qui sont sécurisées. Mais il n'est pas totalement suffisant, car certaines transactions peuvent avoir été libellées comme PDP (Présence Du Porteur) par erreur, voire frauduleusement.

Le second mécanisme utilise les informations décrivant les modalités techniques de lecture des informations du support utilisé par le porteur.

La première est la saisie du code confidentiel, indiqué par le champ 22 (« mode de lecture du système d'acceptation », second sous-champ « capacité de saisie du code »). En effet, dans les systèmes courants, la saisie du code impose une présence physique du porteur. Les exceptions peuvent être traitées en utilisant le champ « mode de lecture du numéro de porteur » (premier sous-champ du champ 22. En effet, il n'y a pas aujourd'hui de système de vente à distance avec à la fois saisie de code et lecture de la piste.

Ce second mécanisme est un filtre très performant des transactions à distance. Toutefois, certaines d'entre elles resteront mal identifiées. Les achats par correspondance payés en utilisant des lecteurs à disposition du porteur (CyberComm, GSM double fente) sont dans ce cas. Pour les identifier correctement, il faut coupler le second mécanisme (saisie du code, lecture de la puce) et le premier (vente à distance).

Les transactions en présence physique du porteur sans lecture de la piste ou de la puce et sans contrôle du code confidentiel pourront être traitées soit comme des transactions à risque (si par exemple elles viennent de pays ou de marchands où le niveau de contrôle de l'identité du porteur et des mécanismes comme l'hologramme sont déficients), soit comme des transactions sûres. En général, on aura intérêt à distinguer, dans le procédé de sélection des transactions à risque, les pays d'origine des transactions.

Enfin, il sera utile d'identifier les transactions issues d'une carte virtuelle dynamique, et de les exclure des mécanismes d'alerte. Ceci peut

se faire soit directement, sur le réseau ou sur le serveur de carte virtuelle, qui disposent tous deux du numéro avec lequel la transaction a été faite (donc le numéro virtuel, reconnaissable par la valeur de ses premiers chiffres). Ceci peut également se faire au niveau de la banque. Dans ce cas, le numéro virtuel peut avoir été remplacé par le numéro réel, mais la mention de l'origine (par exemple la machine ayant fait cette substitution) permet d'identifier que la transaction originelle utilisait un numéro virtuel.

Ces mécanismes de détection s'appliquent lorsque la transaction a fait l'objet d'une demande d'autorisation, ce qui est le cas de la majorité des transactions en vente à distance. En revanche, certaines de ces transactions, soit parce qu'elles sont de montant trop faible, soit plus généralement parce que le marchand n'a pas souhaité faire une telle demande, passent directement au stade du paiement. Dans ce cas, le procédé ici décrit utilise les messages qui parviennent au gestionnaire de paiement de la banque émettrice, qui contiennent essentiellement les mêmes informations que celles utilisées en cas de demande d'autorisation. Bien évidemment, on prévoit de rapprocher les demandes d'autorisation des demandes de paiement, afin qu'une même transaction ne fasse pas l'objet de deux alertes, ce rapprochement étant effectué au moyen des informations de montant et de devise, de pays, de date et, quand ils sont disponibles, de numéro d'autorisation, de marchand, de terminal, etc...

En cas de transactions à risque, les alertes sont envoyées au porteur de la carte, ou plus généralement à une personne ayant un droit de

contrôle sur les dépenses faites avec cette carte. Ce peut être le porteur lui-même, le père ou la mère dans le cas d'un enfant mineur, un chef de service achat dans le cas de cartes d'achat pour les entreprises. Cette personne est désignée dans la suite comme le titulaire.

Les alertes sont envoyées sur un appareil de communication accessible au titulaire. Dans un mode préféré de réalisation de l'invention, cet appareil de communication est un téléphone portable, par exemple un téléphone à la norme GSM ou à une norme similaire. Dans une variante, on utilise des appareils de messagerie (pagers) ou des assistants personnels communicants. Dans une autre variante, on utilise un téléphone fixe, par exemple le téléphone personnel ou le téléphone professionnel du titulaire, ou un télécopieur. Dans une troisième variante, on utilise le courrier électronique, l'appareil de communication étant alors l'ordinateur du titulaire.

Dans ce qui suit, on ne décrira que l'usage d'un téléphone portable, à titre d'exemple, en référence au dessin annexé qui représente schématiquement les principales étapes du procédé selon l'invention.

La constitution d'une liste de correspondance entre numéros de cartes de paiement et numéros de téléphone du titulaire (respectivement de son numéro de messagerie, de son adresse électronique pour les assistants personnels et les courriers électroniques) est un élément essentiel du procédé selon l'invention. Il faut en effet éviter qu'un fraudeur puisse constituer ou modifier une telle liste, par exemple en attribuant à un numéro de carte valide son propre numéro de téléphone. C'est pourquoi cette liste est constituée par les banques des porteurs.

Chaque ligne de la liste fait l'objet d'une garantie par la banque. Cette garantie peut prendre plusieurs formes : certificat numérique pour chaque carte, utilisant un algorithme à clef publique et une clef de la banque; dépôt protégé dans le site de confirmation; dépôt de la liste et protection globale par un certificat à clef publique du site. La banque certifie le lien entre un numéro de carte, représenté par un numéro d'abonné, et le numéro de téléphone portable de l'acheteur (ou de la personne qui est chargée de contrôler ses achats : supérieur hiérarchique ou parent par exemple).

Dans une variante, la liste est constituée et garantie par un opérateur de téléphonie (mobile ou fixe), qui dispose des coordonnées de ses abonnés.

Pour des raisons de sécurité, on préfère stocker les numéros de cartes sous une forme cryptée, avantageusement avec un algorithme de cryptage irréversible. Dans un exemple de fonction de conversion, le numéro de carte, le PAN, est constitué de trois champs : IIN (identification de la banque), AAN (identifiant de la carte) et un chiffre de contrôle CC. On choisit une fonction f irréversible sans collision (par exemple l'algorithme RSA, dont la clef privée a été détruite). Cette fonction est appliquée au PAN et le résultat est concaténé avec le champ IIN pour former un numéro d'abonné. Ensuite, on peut procéder à une certification du numéro d'abonné par sa correspondance avec un identifiant, tel par exemple que le numéro d'appel du téléphone mobile du titulaire. Pour cela, on peut former un couple comportant le numéro d'abonné et le numéro d'appel du téléphone et appliquer aux deux éléments de ce couple une clé de cryptage privée de la banque, pour générer

un certificat.

Le mode d'alerte préféré est le message sur téléphone mobile. Ce message peut être écrit ou vocal. Il est avantageusement conforme à la norme GSM (message SMS, MMS, WAP push). Une variante est le message écrit sur appareil de messagerie. Une autre variante est, pour les porteurs qui disposent d'un tel service, l'utilisation d'une messagerie instantanée, qui choisira automatiquement le mode de transport du message le mieux adapté aux circonstances.

Ce mode d'alerte peut, pour certains porteurs, être remplacé par un message sur téléphone fixe, au numéro personnel ou au numéro professionnel du porteur de carte. On peut prévoir des messages vocaux, mais aussi des messages écrits (qui seront transformés en messages vocaux, ou livrés sous forme écrite sur les écrans des téléphones qui disposent de cette option). Cette variante bénéficiera des futurs services de boites vocales intelligentes, capables de distinguer les membres d'une même famille pour ne livrer les messages qu'aux bons destinataires.

Le message d'alerte comprend les principales informations disponibles permettant au porteur d'identifier la transaction. La forme du message est avantageusement adaptée au mode d'alerte et au canal de communication. Un exemple d'un tel message, conçu pour le mode d'alerte SMS sur GSM est le suivant :

> Alerte sécurité paiement Achat a distance 347F 10/03 carte perso. En cas de fraude tél au '0800 123456'.

Le numéro de téléphone indiqué permet une prise en charge du client. On l'assistera pour vérifier qu'il

conteste bien la transaction, et qu'il ne s'agit pas d'une erreur de sa part. On lui conseillera éventuellement la mise en opposition de sa carte.

Le mode d'alerte préféré est avantageusement complété par un ou des modes d'alerte de secours, pour pallier les cas de défaillance (changement de numéro de téléphone, portable éteint ou hors zone de couverture, défaillance du réseau...). Parmi ces modes de secours on trouvera un autre numéro de téléphone (fixe ou mobile), un message électronique, un télécopieur. Un exemple d'un message de secours est le suivant :

De : service XXX
Objet : achat par carte bancaire non sécurisé
Date : ....
Mr/Mme/Mlle
Nous vous avons alerté, sur votre téléphone portable (numéro 06 XXXX XXXX), après avoir détecté une transaction à distance non sécurisée d'un montant de 347FF faite avec votre carte professionnelle le 10/03/01 (numéro de transaction xxxxxxxxxxxx, abonné yyyyyyyyyy).
N'ayant pas reçu de réponse de votre part, nous nous permettons de vous faire parvenir le présent message.
S'il s'agit d'une transaction frauduleuse, nous vous prions de renvoyer le présent message en mentionnant comme objet 'rejet', puis de remplir le formulaire joint et de l'envoyer, signé, à notre adresse. Ceci nous permettra de traiter votre rejet avec votre banque, et de demander l'ouverture d'une enquête.
Si vous souhaitez faire opposition à votre carte, appelez le 0800 123456.

Si votre numéro de GSM est erroné, veuillez vous connecter au site http://www.mabanque.fr et le modifier.
Vous pourrez disposer d'une assistance téléphonique au 0800 123456 (2FF par minute)

Dans le cas d'une transaction faite par un porteur abonné à un service de carte virtuelle et ayant utilisé son numéro de carte réel, on aura avantage à utiliser un message mentionnant cette possibilité et ses avantages. Cette variante est particulièrement avantageuse si la transaction se prête bien à cette technologie, par exemple si elle est identifiée comme une transaction sur Internet (par exemple si le champ 59 type 200 vaut 24).

Une transaction faite avec un numéro de carte virtuelle peut ne pas être suffisamment sûre, par exemple dans le cas où ce numéro est utilisable plusieurs fois. Une variante consiste alors à envoyer une alerte qui mentionne la carte virtuelle. Un exemple d'un tel message pour le canal SMS est le suivant :

Alerte sécurité paiement Achat internet 347F 10/03 carte perso virtuelle. Pour une fraude aller sur www.mabanque.fr ou tél « 0800 123456 »

Le procédé selon l'invention prévoit plusieurs modes de réponse par le porteur. Le premier mode de réponse est la réponse SMS ou, de manière proche, l'utilisation d'un appareil de messagerie à deux voies. Le message comporte les indications nécessaires (comment, voire vers qui répondre pour confirmer ou rejeter la transaction). Cette réponse

doit être aussi simple que possible. Elle tiendra avantageusement sur une seule lettre (dans l'exemple ci-dessus, 'A' ou 'S'). Elle doit tenir compte des mécanismes de saisie prédictive (sur certains téléphones portables, 'R' est ainsi automatiquement traduit en 'S').

Un autre mode de réponse est la réponse vocale, à un numéro indiqué dans le message ou mis à disposition du porteur par d'autres moyens. Certains téléphones permettent, dans un but de simplicité, l'appel à un numéro mentionné dans le message et reconnu automatiquement.

Le troisième mode de réponse est la réponse écrite, notamment pour les alertes envoyées par courrier électronique ou par télécopieur.

Dans tous les modes de réponse, il faut pouvoir identifier la transaction concernée. En effet, le porteur aura peut-être reçu plusieurs alertes, dont seulement une ou un petit nombre doit être rejetée. Le procédé permet au porteur, en particulier dans les modes de réponse vocaux ou écrits, de donner des précisions sur le transaction pertinente. On prévoit également, en option, de gérer plusieurs émetteurs des messages ou plusieurs numéros de téléphone d'assistance, chaque alerte étant envoyée par un émetteur différent ou mentionnant un numéro d'assistance différent, qui recevra seulement la réponse correspondant à l'alerte qu'il a émise.

Ces émetteurs/numéros de téléphone sont avantageusement utilisés de manière cyclique. Le système dispose d'un nombre suffisant d'émetteurs/numéros de téléphone pour gérer les achats à distance de la grande majorité des porteurs pendant une durée suffisante.

Ces émetteurs peuvent être des émetteurs physiques ou des émetteurs virtuels. Dans le cas des messages GSM, on trouvera naturellement le premier cas si les messages sont envoyés par radio (messages dits MO, Mobile Originated). On dispose alors d'une batterie de modems GSM, chacun identifié par un numéro de téléphone, qui sont gérés de manière cyclique pour chaque titulaire.

Il est avantageux également de prévoir un mode de réponse authentifié par l'acheteur. On peut pour cela demander à l'acheteur, quand il confirme ou quand il conteste la transaction, de saisir un code confidentiel. Ce code peut avantageusement être inscrit dans la carte ou le module SIM inséré dans son téléphone portable. On peut également demander à l'acheteur de répondre via un serveur téléphonique, auquel il indiquera la transaction concernée et donnera son code.

Un rejet d'une transaction par le porteur peut conduire à la mise en œuvre des mécanismes de remboursement prévus par les systèmes bancaires. Par ailleurs, il faut limiter les conséquences de la fraude. Le procédé selon l'invention comporte plusieurs modes de limitation de la fraude.

Un premier mode consiste à identifier le marchand dont la vente est contestée et à l'alerter immédiatement. Si l'alerte a été émise suffisamment rapidement, et si le titulaire a répondu sans délai long, le marchand a la possibilité de ne pas expédier la marchandise. Il pourra également la livrer tout en la maintenant sous surveillance afin de prendre les fraudeurs sur le fait.

Dans ce mode de limitation de la fraude, le marchand est connu grâce aux informations figurant

dans les messages monétiques qui sont des informations d'identification du marchand (par exemple les champs 42 et 43 de la norme ISO 8583), mais également le numéro de terminal (champ 41). On dispose d'une base de données des marchands (ou au moins de certains d'entre eux, dont l'importance dans l'ensemble des ventes à distance est significative), de leurs identifiants, ainsi que des adresses auxquelles envoyer une alerte.

Un avantage de ce mode de limitation de la fraude est qu'il ne nécessite aucune modification du système monétique ou de l'informatique des marchands.

Dans un second mode de limitation de la fraude, complémentaire du premier, on limite l'usage futur de la carte. Dans les procédés traditionnels, ceci prend la forme d'une mise en opposition, puis d'une destruction de la carte. Cette méthode est bien adaptée aux cas classiques de fraude par duplication de carte, mais elle est lourde et coûteuse dans les cas de fraude par utilisation du numéro de carte. Le second mode de limitation de la fraude évite cet inconvénient et consiste à refuser toutes les autorisations comportant le numéro de carte en cause, dès lors qu'il peut s'agir d'une vente en l'absence de la carte physique.

Dans ce mode de limitation de la fraude, on utilise le serveur d'autorisation. Dès qu'une demande d'autorisation comportant le numéro de carte est détectée, on vérifie s'il s'agit d'une vente à distance en utilisant l'un des modes d'identification décrits plus haut. Dans l'affirmative, la demande d'autorisation est refusée, et une alerte est envoyée d'une part au titulaire pour vérifier qu'il n'est pas l'auteur de la transaction, d'autre part à la banque

pour signaler la poursuite de la fraude.

Dans une première réalisation de ce mode de limitation de la fraude, un algorithme de blocage est implanté dans le serveur d'autorisation de la banque.

Dans une seconde réalisation, on utilise un mécanisme de déroutement souvent présent dans les serveurs d'autorisation. Ce mécanisme consulte un liste de numéros de cartes intégrée au serveur. Chaque demande d'autorisation concernant une carte qui fait partie de la liste est déroutée vers une seconde machine, qui peut bloquer ou non la demande. Cette seconde réalisation permet de mettre en place le mécanisme de blocage sans modification logicielle sur la plupart des serveurs d'autorisation.

Dans une troisième réalisation, on dispose d'un serveur dédié dans le réseau interbancaire. C'est lui qui peut détecter les demandes d'autorisation, et prélever celles qui doivent être bloquées.

Ce mode de limitation de la fraude sera avantageusement complété par une intervention au niveau du serveur de paiement. En effet, certaines transactions ne font pas l'objet d'une demande d'autorisation, et le marchand a par ailleurs la possibilité de demander un paiement alors même que l'autorisation de faire la transaction lui a été refusée. Pour ce faire, on inclut dans les algorithmes de paiement un rejet systématique de tout paiement à distance fait avec une carte bloquée. On peut également utiliser une carte de paiement de type "demande d'autorisation au premier franc".

Ceci suppose que le porteur ait formellement indiqué sa volonté de rejeter toute transaction à distance avec son numéro de carte, pour des raisons légales. On pourra avantageusement compléter le rejet

systématique par le serveur de paiement par une diffusion d'une liste de numéros de carte bloqués à destination des vendeurs à distance, analogue à une liste de cartes en opposition.

Dans ces trois réalisations, on peut avantageusement prévoir un mécanisme temporaire d'achat avec un numéro de carte normalement bloqué. Ce mécanisme peut être réalisé de deux manières.

Dans la première réalisation du mécanisme de déblocage temporaire, le porteur qui souhaite faire un achat par correspondance prévient au préalable sa banque. Celle-ci peut alors lever le mécanisme de blocage pendant une durée limitée (par exemple 2 heures), ou pour certains marchands. Dans cette réalisation, un message est envoyé au porteur en cas de demande d'autorisation si la carte n'a pas été débloquée, afin de lui permettre de réparer un éventuel oubli.

Dans la seconde réalisation du mécanisme de blocage temporaire, le porteur qui souhaite faire un achat par correspondance va au préalable chercher, par exemple sur le site internet de sa banque, un numéro de carte temporaire. Il utilise ce numéro, appelé numéro virtuel, en lieu et place du numéro réel. La demande d'autorisation se voit ainsi dirigée vers un serveur particulier, dit serveur de cartes virtuelles, qui remplace le numéro virtuel par le numéro réel, contrôle que l'usage du premier est conforme aux règles qui en limitent l'usage, puis retransmet la demande d'autorisation pour acceptation au serveur de la banque. La demande d'autorisation arrive à la banque munie du numéro réel, ainsi que d'une information qui montre qu'elle a été originellement émise avec un numéro virtuel. Ceci

permet de neutraliser le mécanisme de blocage.

Dans cette réalisation, un message d'alerte est envoyé au porteur même si la transaction a été bloquée. Il indique le motif du rejet, et la possibilité d'utiliser un numéro virtuel. Un exemple d'un tel message pour le canal SMS est le suivant :

> Alerte sécurité paiement Achat a distance 347F 10/03 carte perso refusé. Recommencez l'achat avec numéro virtuel

Ce serveur de cartes virtuelles peut être destinataire de toutes les demandes d'autorisation de la banque, ou ne traiter que les numéros correspondant à des cartes virtuelles. Dans le premier cas, on peut avantageusement prévoir que le serveur de cartes virtuelles est également le serveur de réseau prévu dans la troisième réalisation du mode de limitation de fraude.

REVENDICATIONS

1 - Procédé de sécurisation de transactions effectuées entre des marchands et des acheteurs au moyen de supports d'informations tels que des cartes bancaires et analogues, ce procédé consistant à associer, dans une banque de données protégée, chaque support et un moyen de communication avec le titulaire du support, ce moyen de communication comprenant un téléphone fixe ou mobile ou un appareil analogue, et à faire envoyer par un terminal marchand une demande d'autorisation de transaction ou de paiement à un serveur d'autorisation ou de paiement, cette demande comportant des informations relatives à la transaction et aux modalités de lecture d'informations sur le support utilisé par l'acheteur, caractérisé en ce qu'il consiste également :

- à utiliser lesdites informations incluses dans la demande d'autorisation de transaction ou de paiement pour déterminer si la transaction est à risque ou non,

- si oui, à envoyer au titulaire du support, par le moyen de communication, un message d'alerte lui signalant la transaction à risque, une fois l'autorisation accordée par le banque.

2 - Procédé selon la revendication 1, caractérisé en ce qu'on propose au titulaire du support de mettre le support en opposition.

3 - Procédé selon la revendication 1, caractérisé en ce qu'on propose au titulaire du support de refuser la transaction, et de demander à la banque de recréditer son compte du montant de la transaction.

4 - Procédé selon l'une des revendications 1 à 3,caractérisé en ce que les transactions qui apparaissent comme des ventes à distance sont des transactions à risque.

5 - Procédé selon la revendication 4, caractérisé en ce que les transactions de vente à distance sont identifiées par contrôle des informations définissant les conditions techniques de la transaction telles que le mode de lecture du numéro de support ou le contrôle d'un code confidentiel.

6 - Procédé selon la revendication 4 ou 5, caractérisé en ce que les transactions de vente à distance sont identifiées par contrôle des conditions réglementaires ainsi que par corrélation avec la disponibilité du résultat de la lecture de la piste magnétique ou de la puce du support.

7 - Procédé selon l'une des revendications 4 à 6, caractérisé en ce que dans la détection des ventes à distance, on prend en compte le pays d'origine de la transaction.

8 - Procédé selon l'une des revendications 1 à 7, caractérisé en ce que le moyen de communication avec le titulaire du support est un téléphone fixe ou mobile ou un appareil de messagerie ou un assistant personnel communicant, ou un courrier électronique.

9 - Procédé selon l'une des revendications 1 à 8, caractérisé en ce que le message d'alerte est un message écrit ou vocal.

10 - Procédé selon l'une des revendications précédentes, caractérisé en ce que le moyen de communication comporte une voie principale et au moins une voie secondaire utilisée en cas de défaillance ou de délai dans la voie principale.

11 - Procédé selon l'une des revendications précédentes, caractérisé en ce que le message d'alerte comporte des indications données au titulaire sur la manière de répondre.

12 - Procédé selon l'une des revendications précédentes, caractérisé en ce que les messages d'alerte sur les transactions par un même titulaire sont envoyées par des émetteurs différents qui reçoivent uniquement les réponses aux messages qu'ils ont émis.

13 - Procédé selon la revendication 8, caractérisé en ce que la réponse tient en un seul caractère, non modifiable par l'algorithme de saisie prédictif d'un téléphone mobile.

14 - Procédé selon l'une des revendications précédentes, caractérisé en ce que le rejet d'une transaction par le titulaire déclenche un blocage par un serveur d'autorisation des transactions à distance ultérieures utilisant le même support.

15 - Procédé selon la revendication 14, caractérisé en ce que le serveur d'autorisation comporte un algorithme de blocage.

16 - Procédé selon la revendication 14, caractérisé en ce que le serveur d'autorisation déroute les demandes dont le support appartient à une liste vers une seconde machine qui les bloque.

17 - Procédé selon l'une des revendications 14 à 16, caractérisé en ce que le serveur d'autorisation

qui bloque les transactions est dans le réseau interbancaire.

18 - Procédé selon l'une des revendications 14 à 16, caractérisé en ce que le blocage des transactions à distance est temporairement désactivable par une action volontaire du titulaire du support.

19 - Procédé selon l'une des revendications 14 à 16, caractérisé en ce que le blocage des transactions à distance peut être contourné en utilisant un numéro de support virtuel, que le mécanisme de blocage ne reconnaît pas, et qui est ensuite remplacé par le numéro réel du support.

20 - Procédé selon la revendication 19, caractérisé en ce qu'une transaction à distance faite avec un numéro de support virtuel déclenche l'émission d'un message spécifique vers le titulaire du support.

21 - Procédé selon la revendication 19, caractérisé en ce que le mécanisme de blocage et le mécanisme de cartes virtuelles sont gérés par les mêmes machines.

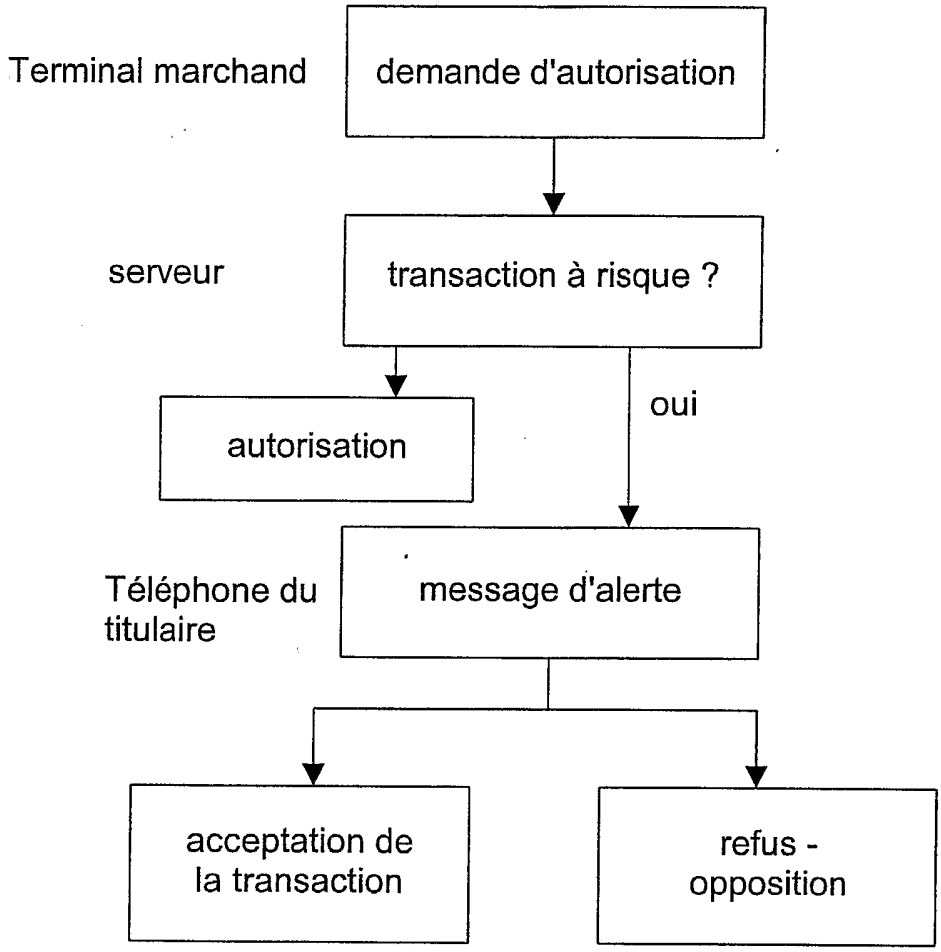
22 - Procédé selon l'une des revendications 14 à 21, caractérisé en ce que le mécanisme de blocage est également réalisé dans le serveur de paiement.

23 - Procédé selon l'une des revendications 14 à 22, caractérisé en ce qu'une liste des numéros de supports bloqués est diffusée à un ensemble de sites de vente à distance.

24 - Procédé selon l'une des revendications 14 à 23, caractérisé en ce qu'il existe une base de données de marchands par correspondance et de leurs identifiants dans les transactions monétiques, et en ce que tout rejet par le titulaire d'une transaction

comportant un de ces identifiants fait l'objet d'une information rapide du marchand, avant finalisation de la livraison.

25 - Procédé selon l'une des revendications 18 à 24, caractérisé en ce qu'une transaction à distance faite avec un support bloqué déclenche l'émission d'un message vers le titulaire du support, lui recommandant d'utiliser un numéro de support virtuel à la place du numéro réel du support.


Terminal marchand
demande d'autorisation
serveur
transaction à risque ?
autorisation
oui
Téléphone du titulaire
message d'alerte
acceptation de la transaction
refus - opposition