(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 026 525**

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

(21) **N° d'enregistrement national :** **14 59134**

(51) Int Cl[8] : ***G 06 F 21/60*** *(2016.01), G 06 F 21/44*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 26.09.14.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 01.04.16 Bulletin 16/13.

(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) :** *COMPAGNIE INDUSTRIELLE ET FINANCIERE D'INGENIERIE "INGENICO"* — FR.

(72) **Inventeur(s) :** NACCACHE DAVID et MAYER LAURENT.

(73) **Titulaire(s) :** COMPAGNIE INDUSTRIELLE ET FINANCIERE D'INGENIERIE "INGENICO".

(74) **Mandataire(s) :** CABINET PATRICE VIDON.

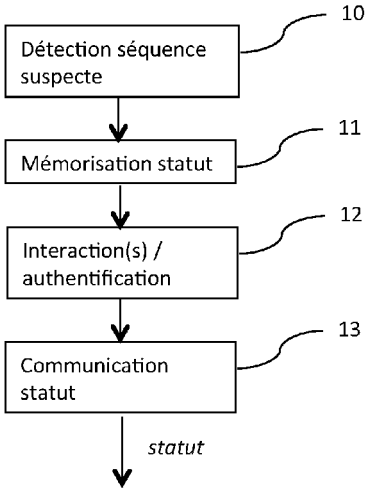
(54) PROCEDE D'AUTO-DETECTION D'UNE TENTATIVE DE PIRATAGE D'UNE CARTE ELECTRONIQUE DE PAIEMENT, CARTE, TERMINAL ET PROGRAMME CORRESPONDANTS.

(57) L'invention concerne un procédé d'auto-détection d'une tentative de piratage d'une carte électronique de paiement, comprenant les étapes suivantes, mises en oeuvre par ladite carte:

détection (10) d'une séquence d'opérations suspectes mises en oeuvre en interaction avec ladite carte et mémorisation (11), dans ladite carte, d'un statut correspondant, dit statut suspect;

interaction (12) de ladite carte avec une entité distincte et authentification (12), par ladite carte, de ladite entité distincte;

communication (13), par ladite carte, dudit statut suspect mémorisé à ladite entité distincte authentifiée.



FR 3 026 525 - A1

Procédé d'auto-détection d'une tentative de piratage d'une carte électronique de paiement, carte, terminal et programme correspondants

1. Domaine de l'invention

L'invention se rapporte au domaine du paiement électronique et plus particulièrement à la sécurisation des cartes électroniques de paiement.

2. Art Antérieur

Les cartes de paiement font l'objet de nombreuses tentatives d'attaques. En effet, de par la nature des informations qu'elle contient et la sensibilité des données qu'elle permet de traiter, la carte électronique de paiement est un objet qui possède une grande valeur pour des personnes malveillantes.

Un certain type de fraude tend à prendre de l'ampleur : il s'agit du « *skimming* », opération frauduleuse qui consiste d'abord à effectuer une copie de la bande magnétique de la carte à l'aide d'un dispositif spécial sans que le possesseur de la carte ne le remarque, par exemple lorsque la carte est insérée dans un distributeur automatique de billets. Ces données sont ensuite reportées sur une carte vierge pour une utilisation ultérieure. Parallèlement, les fraudeurs ont également récupéré le code confidentiel saisi par le possesseur de la carte, par exemple à l'aide d'une caméra cachée ou d'un dispositif placé sur ou sous le clavier du distributeur automatique de billets.

Une fois en possession de la carte falsifiée et du code confidentiel, les fraudeurs peuvent ainsi effectuer des transactions ou même accéder au compte bancaire de l'utilisateur. Et comme l'utilisateur n'a rien remarqué et qu'il est toujours en possession de la carte d'origine, ce n'est qu'au moment de consulter le solde de son compte qu'il remarquera qu'il est victime d'escroquerie.

Ainsi, pour pirater et cloner une carte bancaire, un fraudeur a besoin de deux types d'information : les données stockées sur la carte (coordonnées bancaires) et le code confidentiel personnel à 4 chiffres.

Une solution pour lutter contre ce type de fraude consiste à tenter de détecter les dispositifs piratés, comme les distributeurs automatiques de billets, par exemple en informant les utilisateurs de façon précise pour qu'ils puissent reconnaître lorsqu'un distributeur a été piraté (par exemple lorsque la fente d'insertion de la carte paraît suspecte). Cette solution n'est en revanche pas très efficace, dans la mesure où les fraudeurs prennent de plus en plus de précautions pour ne pas être détectés.

Une autre solution, également à mettre en œuvre par l'utilisateur, consiste à prendre plus de précautions lors de la saisie d'un code confidentiel, en mettant la main au-dessus du clavier par exemple, de manière à déjouer une partie du piratage basée sur la caméra filmant la saisie du code. De la même manière, cette solution n'est pas très efficace dans la mesure où l'utilisateur ne sait pas où se trouve cette caméra et dans la mesure où tous les utilisateurs ne pensent pas à prendre ce type de précautions.

Les techniques existantes sont donc limitées à la détection de dispositifs piratés ou à la vigilance des utilisateurs pour déjouer de telles fraudes.

Il existe donc un besoin de fournir une technique qui permette de détecter une fraude/tentative de fraude par modification d'une carte bancaire d'un utilisateur et qui permette de se prémunir des effets négatifs d'une telle fraude.

3. Résumé de l'invention

L'invention propose une solution nouvelle qui ne présente pas l'ensemble de ces inconvénients de l'art antérieur, sous la forme d'un procédé d'auto-détection d'une tentative de piratage d'une carte électronique de paiement, comprenant les étapes suivantes, mises en œuvre par la carte :

- détection d'une séquence d'opérations suspectes mises en œuvre en interaction avec la carte et mémorisation, dans la carte, d'un statut correspondant, dit statut suspect ;
- interaction de la carte avec une entité distincte et authentification, par la carte, de l'entité distincte ;
- communication, par la carte, du statut suspect mémorisé à l'entité distincte authentifiée.

Ainsi, l'invention propose une solution nouvelle et inventive de la détection de fraude à la carte bancaire mettant notamment en œuvre le piratage par copie des données d'une carte bancaire (ainsi que l'obtention du code confidentiel correspondant), basée sur l'auto-détection, par la carte elle-même, d'une tentative de piratage.

Pour ce faire, la carte bancaire détecte elle-même que des opérations mises en œuvre par le fraudeur (consistant à lire les données de la carte sans toutefois mettre en œuvre une transaction complète) sont suspectes et mémorise un statut particulier représentatif d'une tentative de piratage.

Ensuite, lorsque la même carte est utilisée par un dispositif authentique, la carte communique son statut suspect, de façon à ce que l'utilisateur de la carte ou du dispositif soit alerté.

De cette manière, si l'utilisateur n'a pas détecté le dispositif frauduleux (par exemple un distributeur automatique de billets modifié) permettant un piratage de sa carte bancaire par copie des données de la carte et obtention via une caméra de son code confidentiel lors de sa saisie, la solution proposée permet de détecter ce piratage dès l'utilisation suivante de la carte piratée.

L'utilisateur est alors informé que sa carte est piratée et qu'il doit contacter sa banque pour la bloquer et empêcher d'ultérieures utilisations frauduleuses.

La solution proposée n'est donc pas basée, contrairement aux techniques préventives peu efficaces de l'art antérieur, sur la détection de dispositifs modifiés pour permettre un piratage, mais elle est basée sur l'auto-détection par la carte elle-même d'une tentative de piratage ou d'un piratage avéré.

Selon une caractéristique particulière de l'invention, l'étape de détection d'une séquence d'opérations suspectes comprend la détection d'une séquence d'opérations ne correspondant pas à une séquence prédéterminée d'opérations permettant la réalisation complète d'une transaction bancaire.

Ainsi, selon ce mode de réalisation particulier, la carte bancaire détecte elle-même que les opérations mises en œuvre par le fraudeur ne correspondent pas à une séquence complète d'opérations nécessaires à la réalisation d'une transaction et sont donc suspectes.

En effet, toutes les opérations autorisées pour une carte de paiement électronique sont connues et normalisées, et permettent notamment la finalisation d'une transaction. Ainsi, lorsque seulement certaines des opérations appartenant à une séquence de transaction sont mises en œuvre, la carte peut détecter un comportement anormal et donc mémoriser un statut suspect, représentatif d'une tentative de piratage.

Par exemple, l'entité distincte correspond à un terminal de paiement électronique et l'étape d'authentification correspond à une étape de mise en œuvre d'une transaction complète via le terminal de paiement électronique.

Ainsi, selon ce mode de réalisation particulier, la carte bancaire est capable d'authentifier elle-même une entité distincte, par exemple un terminal de paiement électronique.

En effet, lorsqu'une transaction complète est mise en œuvre, dans un terminal de paiement électronique, avec la carte, celle-ci en déduit que le terminal de paiement électronique est authentique et qu'elle peut lui communiquer son statut particulier (préalablement mémorisé) représentatif d'une tentative de fraude, pour l'alerter.

Ainsi, lorsque la carte préalablement piratée est utilisée, de manière classique, pour une transaction complète via un terminal de paiement électronique authentique, la carte, encore insérée dans le terminal de paiement électronique, déclenche la communication de son statut suspect vers le terminal de paiement électronique.

Selon un aspect particulier de l'invention, l'étape de détection est sécurisée et la mémorisation du statut suspect est garantie quelles que soient les opérations mises en œuvre.

Ainsi, selon ce mode de réalisation particulier, la carte bancaire peut détecter une séquence d'opérations suspectes quelles que soient ces opérations, y compris si elles incluent une remise à zéro de certaines données de la carte.

En effet, la mémorisation du statut suspect concerne une zone protégée de la mémoire de la carte.

Par exemple, l'étape de communication comprend une sous-étape de transmission d'au moins une commande d'affichage d'un message d'alerte sur un écran de l'entité distincte.

Ainsi, selon ce mode de réalisation particulier, la communication de son statut suspect par la carte permet par exemple d'afficher directement une alerte sur l'écran du terminal de paiement électronique dans lequel la carte est insérée, ou avec lequel la carte a mis en œuvre la transaction complète.

De cette manière, l'utilisateur porteur de la carte piratée et/ou le commerçant en possession du terminal de paiement électronique, peut visualiser le message d'alerte et ainsi être informé d'une possible tentative de piratage de la carte.

Selon une caractéristique particulière de l'invention, le procédé comprend une étape de traitement, dans l'entité distincte, du statut suspect communiqué par la carte.

Ainsi, selon ce mode de réalisation particulier, l'entité authentifiée ayant reçu le statut représentatif d'une tentative de fraude par la carte met en œuvre une étape de traitement de ce statut, afin d'alerter le porteur de la carte par exemple, ou bien l'utilisateur de l'entité authentifiée (le commerçant utilisant un terminal de paiement électronique).

Par exemple, le traitement du statut entraine l'affichage d'un message d'alerte sur un écran de l'entité authentifiée, ou encore génère l'émission d'un signal sonore d'alerte.

Selon un autre exemple, ce traitement consiste à émettre un message à destination d'un serveur distant (par exemple le serveur bancaire avec lequel la transaction précédente a été effectuée), ce serveur informant ensuite directement le porteur de la carte ou l'utilisateur de l'entité authentifiée de la tentative de fraude sur la carte.

L'invention concerne également une carte électronique de paiement comprenant des moyens d'auto-détection d'une tentative de piratage, et les moyens suivants :

- moyens de détection, par exemple sous la forme d'un module de détection, d'une séquence d'opérations suspectes mises en œuvre en interaction avec la carte et moyens de mémorisation, par exemple sous la forme d'un module de mémorisation, dans la carte, d'un statut correspondant, dit statut suspect ;
- moyens d'interaction, par exemple sous la forme d'un module d'interaction, de la carte avec une entité distincte et moyens d'authentification, par exemple sous la forme d'un module d'authentification, par la carte, de l'entité distincte ;
- moyens de communication, par exemple sous la forme d'un module de communication, par la carte, du statut suspect mémorisé à l'entité distincte authentifiée.

L'invention concerne également un terminal de paiement électronique comprenant des moyens de traitement d'un statut suspect reçu en provenance d'une carte électronique de paiement.

Enfin, l'invention concerne un produit programme d'ordinateur téléchargeable depuis un réseau de communication et/ou stocké sur un support lisible par ordinateur et/ou exécutable par un microprocesseur, et comprenant des instructions de code de programme pour l'exécution d'un procédé d'auto-détection tel que décrit précédemment, lorsqu'il est exécuté sur un ordinateur.

4. Figures

D'autres caractéristiques et avantages de l'invention apparaîtront plus clairement à la lecture de la description suivante d'un mode de réalisation préférentiel, donné à titre de simple exemple illustratif et non limitatif, et des dessins annexés, parmi lesquels :

- la figure 1 présente un synoptique de la technique proposée, selon un mode de réalisation particulier ;
- la figure 2 présente un diagramme de séquences de la technique proposée, selon un mode de réalisation particulier ;
- les figures 3a et 3b présentent deux exemples d'une carte de paiement électronique selon un mode de réalisation particulier de la technique proposée ;
- la figure 4 présente un exemple d'un terminal de paiement selon un mode de réalisation particulier de la technique proposée.

5. Description

5.1. Principe général

Le principe général de la technique proposée, décrit en relation avec les figures 1 et 2, est basé sur l'auto-détection, par une carte de paiement électronique, d'une fraude ou tentative de fraude sur cette carte et sur la mémorisation, par la carte, d'un statut suspect en vue de sa communication ultérieure à une entité distincte préalablement authentifiée.

Ainsi, la carte de paiement électronique est capable de détecter des interactions suspectes entre une entité distincte et elle-même, et de mémoriser un état/statut suspect y relatif. Ensuite, lorsque la même carte est utilisée dans une entité qu'elle est capable d'authentifier, la carte communique à cette entité son statut suspect, de façon à alerter un ou plusieurs utilisateurs de la tentative de fraude (ou de la fraude avérée).

Pour ce faire, la carte de paiement électronique comprend des moyens spécifiques, selon les différents modes de réalisation décrits ci-après.

5.2. Description de modes de réalisation

On décrit maintenant, en relation avec la figure 1, les principales étapes du procédé d'auto-détection mises en œuvre dans une carte de paiement électronique, selon un mode de réalisation particulier de l'invention.

La première étape de détection 10 consiste à détecter, par la carte elle-même, une séquence d'opérations/interactions suspectes, par exemple lorsque cette carte est insérée dans un terminal de paiement électronique, un accessoire de paiement ou un distributeur de billets.

Par exemple, cette séquence d'opérations jugées suspectes correspond à une partie seulement des opérations prédéterminées (par exemple les étapes d'une transaction telle que définies par la norme EMV, pour « Europay Mastercard Visa ») nécessaires à la mise en œuvre d'une transaction bancaire. Ainsi, la carte de paiement électronique selon ce mode de réalisation de l'invention détecte une séquence suspecte lorsqu'un arrêt est détecté dans une quelconque des étapes prédéterminées obligatoires. Une telle séquence considérée comme suspecte entraine la mémorisation, lors d'une étape 11, par la carte elle-même, d'un statut suspect.

Par exemple, cette mémorisation 11 consiste à modifier un bit de statut dans une partie spécifique de la mémoire de la puce électronique de la carte ou à mémoriser une suite particulière de bits (correspondant à des commandes à exécuter par le dispositif récepteur de cette suite de bits par exemple) dans une partie spécifique de la mémoire de la puce électronique de la carte.

Selon ce mode de réalisation particulier de l'invention, la mémorisation du statut suspect de la carte est toujours possible, quelles que soient les opérations mises en œuvre sur la carte.

Ainsi, si la fraude consiste à copier puis effacer tout ou partie de la mémoire de la carte, la zone de mémorisation du statut suspect est sauvegardée. Par exemple, cette mémorisation est effectuée dans une zone spécifique de la mémoire non accessible à un éventuel fraudeur, ou non effaçable.

Ce mode de réalisation constitue seulement un exemple de réalisation, non limitatif et il est clair que de nombreux autres modes de réalisation de l'invention peuvent être envisagés pour mémoriser le statut par la carte.

Une fois le statut mémorisé, la carte de paiement électronique peut alors le communiquer, le cas échéant, à tout dispositif de confiance, de façon à alerter un utilisateur, par exemple le porteur de la carte, de la fraude ou tentative de fraude.

Par exemple, lorsque la carte de paiement électronique est utilisée, après la tentative de piratage, par un utilisateur, dans un terminal de paiement électronique ou un distributeur de billets, la carte communique son statut suspect, dès lors qu'elle est en mesure d'authentifier le dispositif en question.

Pour ce faire, lorsque la carte est à nouveau en interaction avec une entité distincte, elle met en œuvre une étape 12 d'authentification de cette entité, afin de pouvoir ensuite, lors d'une étape 13, lui communiquer son statut suspect.

Par exemple, lorsque la carte détecte cette fois qu'une transaction bancaire complète est mise en œuvre avec l'entité distincte, cette dernière est considérée comme authentique par la carte. En effet, un terminal de paiement électronique, ou un distributeur de billets, permettant une transaction bancaire complète peut être considéré comme authentique et de confiance par la carte de paiement électronique. Une telle entité authentifiée permet de plus la communication du statut suspect de la carte, voire même une alerte immédiate via les moyens d'affichage de cette entité.

Ainsi, lors de l'utilisation de la carte bancaire (pour une transaction dans un terminal de paiement électronique ou un retrait d'argent dans un distributeur de billets), la carte de paiement électronique piratée « profite » de son interaction avec une entité distincte qu'elle juge authentique pour communiquer son statut suspect (mémorisé antérieurement lors d'un piratage ou une tentative de piratage).

Ensuite, l'entité distincte ayant reçu cette communication de statut suspect de la carte de paiement électronique met en œuvre une ou plusieurs étapes permettant de tenir compte de ce statut suspect pour émettre une alerte.

Par exemple, la réception du statut suspect en provenance de la carte déclenche automatiquement l'affichage, par des moyens de restitution de l'entité distincte (l'écran d'un terminal de paiement électronique), d'un message d'alerte indiquant que la carte a subi une tentative de piratage ou un piratage et qu'elle doit être vérifiée.

Selon un autre exemple, la lecture du statut suspect communiqué déclenche l'exécution d'une ou plusieurs commandes permettant l'affichage, par des moyens de restitution de l'entité distincte, d'un message d'alerte indiquant que la carte a subi une tentative de piratage ou un piratage et qu'elle doit être vérifiée.

Selon encore un autre exemple, la lecture du statut suspect communiqué déclenche l'exécution d'une ou plusieurs commandes permettant la transmission, par l'entité distincte, à un serveur distant (par exemple le serveur de l'organisme bancaire émetteur de la carte) ou un dispositif préalablement identifié (par exemple le téléphone portable du porteur de la carte), d'une alerte, de façon à informer un utilisateur préalablement identifié (le porteur de la carte par exemple).

Les étapes décrites ci-dessus sont également illustrées en figure 2, sous la forme d'un diagramme de séquences impliquant un dispositif piraté 22, la carte de paiement électronique 20 objet de l'invention et une entité distincte authentifiée 21.

Selon un mode de réalisation particulier de l'invention, la carte de paiement électronique 20 détecte une séquence d'opérations suspectes, en interaction avec un dispositif 22 (par exemple un distributeur de billets piraté). Par exemple, la carte détecte que seulement certaines des étapes nécessaires à la mise en œuvre d'une transaction bancaires sont mises en œuvre et en déduit qu'elle subit un piratage ou une tentative de piratage. Elle mémorise alors un statut particulier dit « suspect », afin de pouvoir ensuite, dès que possible, communiquer ce statut à une entité apte à alerter de cette tentative de piratage.

Ainsi, lorsque la carte 20 entre à nouveau en interaction avec une entité distincte 21 (un distributeur de billets, un terminal de paiement électronique, un accessoire de paiement ...), elle s'assure de son authenticité pour ensuite lui communiquer son statut suspect.

Par exemple, la carte 20 déduit que le terminal de paiement électronique 21 dans lequel elle est insérée est authentique lorsqu'une transaction bancaire complète a été mise en œuvre, c'est-à-dire lorsque toutes les étapes/opérations prédéterminées nécessaires à une transaction ont été effectuées. Dès lors que l'entité distincte 21 en interaction avec la carte 20 est authentifiée, cette dernière peut lui communiquer son statut suspect.

L'entité distincte 21 authentifiée peut alors traiter ce statut suspect de façon à générer une alerte, en affichant un message sur son écran par exemple, ou en émettant un message d'alerte à destination d'un serveur distant ou d'un dispositif préalablement identifié (par exemple le téléphone portable du porteur de carte).

Ainsi, selon les différents modes de réalisation décrits précédemment, l'invention permet l'auto-détection, par une carte de paiement, d'un piratage ou d'une tentative de piratage et la communication, dès que possible, à une entité distincte authentifiée, d'un statut suspect mémorisé par la carte.

La fraude est donc détectée par la carte elle-même et divulguée rapidement (dès l'utilisation suivante de la carte pour un paiement par exemple) de façon à permettre à l'utilisateur de prendre les mesures nécessaires pour que le piratage ait le moins d'effets négatifs possibles. En effet, si l'utilisateur est alerté rapidement après le piratage, il peut y mettre fin sans attendre, alors qu'actuellement il ne peut se rendre compte de la fraude que lorsqu'il consulte son compte et que de nombreuses transactions frauduleuses ont potentiellement déjà été effectuées.

5.3. Autres caractéristiques et avantages

On décrit, en relation avec les figures 3a et 3b, un exemple de carte de paiement électronique comprenant des moyens d'exécution du procédé d'auto-détection d'une tentative de piratage décrit préalablement.

Ainsi, comme illustré en figure 3a, une telle carte de paiement électronique 20 comprend des moyens de détection 30 d'une séquence d'opérations suspectes. La carte de paiement électronique 20 comprend également des moyens de mémorisation 31 d'un statut suspect, lorsqu'une séquence suspecte a été détectée. La carte de paiement électronique 20 comprend également des moyens d'interaction et d'authentification 32 ainsi que des moyens de communication 33 du statut préalablement mémorisé par les moyens 31.

On décrit maintenant cette carte de paiement électronique 20 en relation avec la figure 3b.

Par exemple, la carte de paiement électronique 20 comprend une mémoire 201 constituée d'une mémoire tampon, une unité de traitement 202, équipée par exemple d'un microprocesseur, et pilotée par le programme d'ordinateur 203, mettant en œuvre le procédé d'auto-détection d'une tentative de piratage tel que décrit précédemment.

À l'initialisation, les instructions de code du programme d'ordinateur 203 sont par exemple chargées dans une mémoire avant d'être exécutées par le processeur de l'unité de traitement 202. L'unité de traitement 202 reçoit en entrée par exemple une séquence d'opérations, en interaction la carte 20. Le microprocesseur de l'unité de traitement 202 met en œuvre les étapes du procédé d'auto-détection d'une tentative de piratage, selon les instructions du programme d'ordinateur 203, pour communiquer un statut suspect.

Pour cela, la carte de paiement électronique 20 comprend, outre la mémoire tampon 201, des moyens de détection 30 d'une séquence d'opérations suspectes, des moyens de mémorisation 31 d'un statut suspect, lorsqu'une séquence suspecte a été détectée, des moyens d'interaction et d'authentification 32 ainsi que des moyens de communication 33 du statut préalablement mémorisé par les moyens 31.

On décrit enfin, en relation avec la figure 4, un exemple de terminal de paiement électronique 21 comprenant des moyens de traitement 40 d'un statut reçu en provenance d'une carte de paiement mettant en œuvre le procédé d'auto-détection d'une tentative de piratage selon les différents modes de réalisation particuliers de l'invention.

Ces moyens de traitement 40 comprennent par exemple des moyens de lecture du statut reçu, des moyens d'exécution de commande(s) comprises dans le statut reçu, comme par exemple des moyens d'affichage d'une alerte ou d'émission d'un message d'alerte vers une autre entité distante.

Revendications

1. Procédé d'auto-détection d'une tentative de piratage d'une carte électronique de paiement, caractérisé en ce qu'il comprend les étapes suivantes, mises en œuvre par ladite carte :

- détection (10) d'une séquence d'opérations suspectes mises en œuvre en interaction avec ladite carte et mémorisation (11), dans ladite carte, d'un statut correspondant, dit statut suspect ;
- interaction (12) de ladite carte avec une entité distincte et authentification (12), par ladite carte, de ladite entité distincte ;
- communication (13), par ladite carte, dudit statut suspect mémorisé à ladite entité distincte authentifiée.

2. Procédé d'auto-détection selon la revendication 1, caractérisé en ce que ladite étape de détection d'une séquence d'opérations suspectes comprend la détection d'une séquence d'opérations ne correspondant pas à une séquence prédéterminée d'opérations permettant la réalisation complète d'une transaction bancaire.

3. Procédé d'auto-détection selon les revendications 1 ou 2, caractérisé en ce que ladite entité distincte correspond à un terminal de paiement électronique et en ce que ladite étape d'authentification correspond à une étape de mise en œuvre d'une transaction complète via ledit terminal de paiement électronique.

4. Procédé de détection selon l'une quelconque des revendications 1 à 3, caractérisé en ce que ladite étape de détection est sécurisée et ladite mémorisation dudit statut suspect est garantie quelles que soient lesdites opérations mises en œuvre.

5. Procédé de détection selon l'une quelconque des revendications 1 à 4, caractérisé en ce que ladite étape de communication comprend une sous-étape de transmission d'au moins une commande d'affichage d'un message d'alerte sur un écran de ladite entité distincte.

6. Procédé de détection selon l'une quelconque des revendications 1 à 5, caractérisé en ce qu'il comprend une étape de traitement, dans ladite entité distincte, dudit statut suspect communiqué par ladite carte.

7. Carte électronique de paiement comprenant des moyens d'auto-détection d'une tentative de piratage, caractérisée en ce qu'elle comprend les moyens suivants :

- moyens (30) de détection d'une séquence d'opérations suspectes mises en œuvre en interaction avec ladite carte et moyens (31) de mémorisation, dans ladite carte, d'un statut correspondant, dit statut suspect ;
- moyens (32) d'interaction de ladite carte avec une entité distincte et moyens (32) d'authentification, par ladite carte, de ladite entité distincte ;
- moyens (33) de communication, par ladite carte, dudit statut suspect mémorisé à ladite entité distincte authentifiée.

8. Terminal de paiement électronique comprenant des moyens de traitement d'un statut suspect reçu en provenance d'une carte électronique de paiement selon la revendication 7.

9. Produit programme d'ordinateur téléchargeable depuis un réseau de communication et/ou stocké sur un support lisible par ordinateur et/ou exécutable par un microprocesseur, caractérisé en ce qu'il comprend des instructions de code de programme pour l'exécution d'un procédé selon l'une quelconque des revendications 1 à 6, lorsqu'il est exécuté sur un ordinateur.

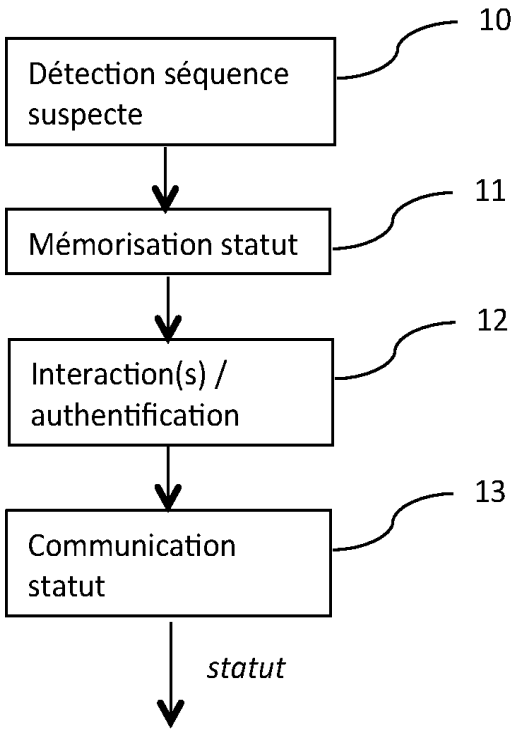


Figure 1

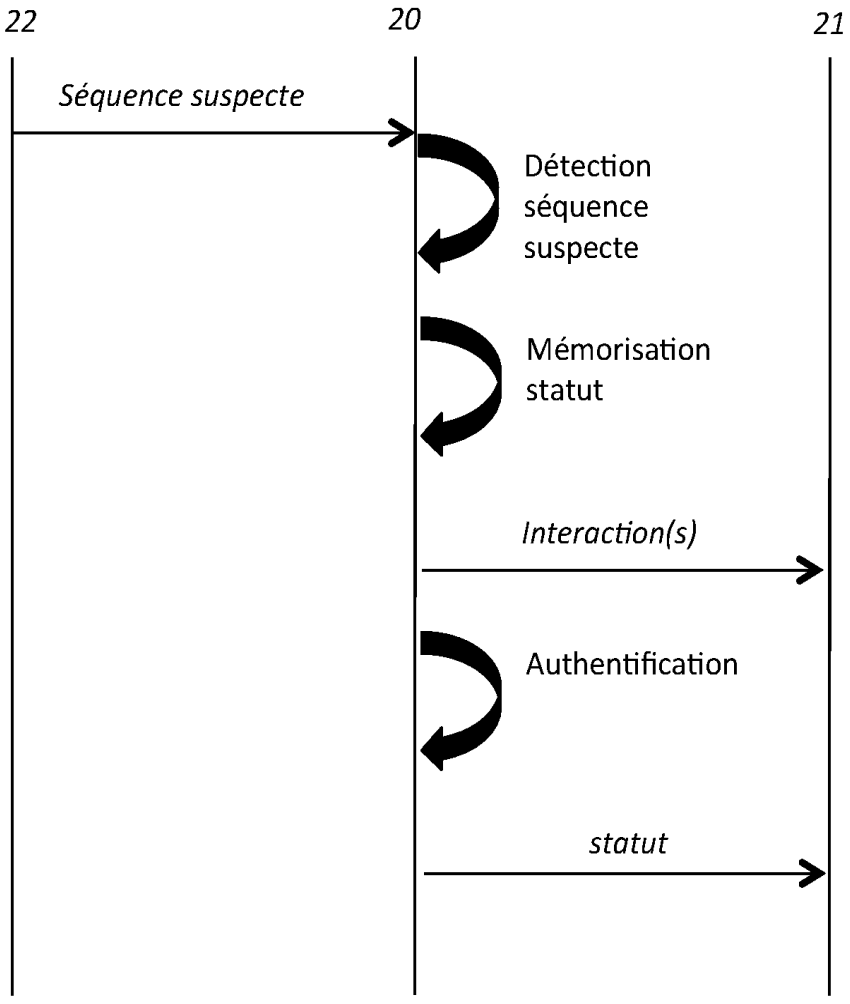


Figure 2

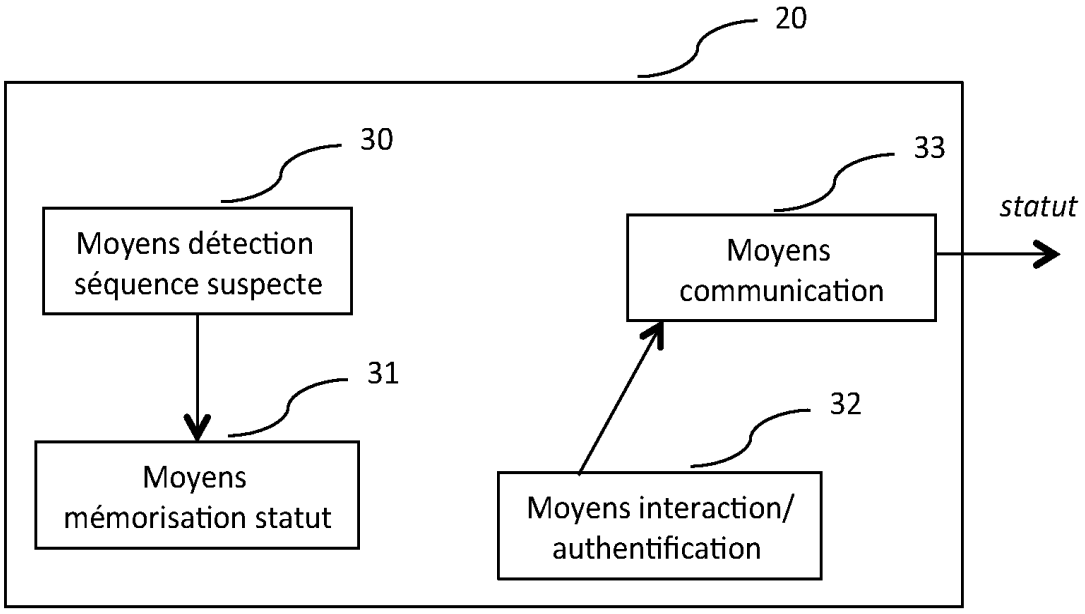


Figure 3a

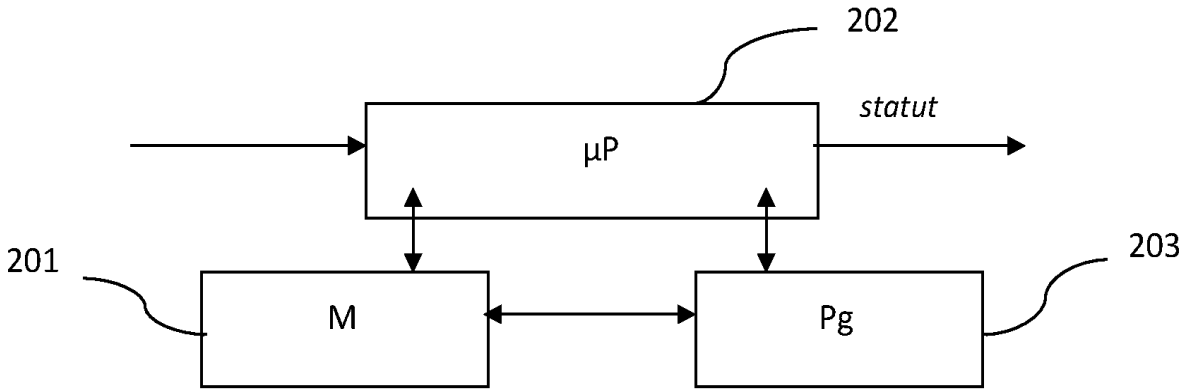


Figure 3b

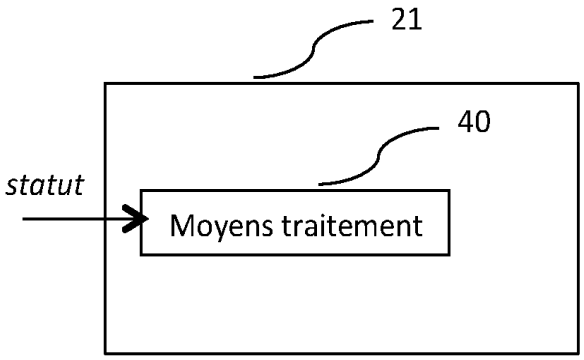


Figure 4

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 806516
FR 1459134

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	EP 2 085 921 A1 (INTELLIGENT WAVE INC [JP]) 5 août 2009 (2009-08-05) * alinéas [0040], [0061] - [0064], [0073], [0074], [0107]; figure 4 * -----	1-9	G06F21/60 G06F21/44
			DOMAINES TECHNIQUES RECHERCHÉS (IPC) G06Q G07F

Date d'achèvement de la recherche	Examinateur
31 août 2015	Manea, Anda

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 1459134 FA 806516

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 31-08-2015
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
EP 2085921 A1	05-08-2009	EP 2085921 A1	05-08-2009
		JP 4173532 B1	29-10-2008
		US 2010327056 A1	30-12-2010
		WO 2009069202 A1	04-06-2009

EPO FORM P0465