(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **2 999 751**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **12 62038**

(51) Int Cl[8] : ***G 06 F 21/70*** *(2017.01)*

(12) BREVET D'INVENTION B1

(54) PROCEDE DE PROTECTION D'UN TERMINAL ELECTRONIQUE, PROGRAMME D'ORDINATEUR, ET TERMINAL ELECTRONIQUE CORRESPONDANTS.

(22) **Date de dépôt :** 14.12.12.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 20.06.14 Bulletin 14/25.

(45) **Date de la mise à disposition du public du brevet d'invention :** 02.02.18 Bulletin 18/05.

(56) **Liste des documents cités dans le rapport de recherche :**

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) :** VOELCKEL JEAN-MARC et SOUSSANA ISAAC.

(73) **Titulaire(s) :** INGENICO GROUP.

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

FR 2 999 751 - B1

Procédé de protection d'un terminal électronique, programme d'ordinateur, et terminal électronique correspondants.

1. Domaine de l'invention

Le domaine de l'invention est celui des terminaux électroniques, et notamment des terminaux électroniques destinés à manipuler des données sensibles, par exemple des terminaux de paiement électroniques ou des terminaux destinés à lire et/ou à mettre à jour des cartes électroniques contenant des données médicales personnelles (comme une carte vitale en France) et/ou à déclarer des actes médicaux auprès d'un organisme de santé. Le domaine de l'invention concerne plus particulièrement la lutte contre le vol ou le détournement à des fins malveillantes de tels terminaux.

2. Art antérieur

Du fait de la nature des opérations auxquelles ils sont destinés, les terminaux manipulant des données sensibles, liées en particulier à des aspects monétaires, comme les terminaux de paiement électroniques, constituent des cibles préférentielles d'agressions informatiques.

Ils peuvent souvent faire l'objet de vols, qui ont notamment pour but l'installation d'un composant parasite au sein du terminal.

En particulier, un tel composant peut avoir pour but de nuire à la disponibilité ou au fonctionnement de ce terminal, ou d'utiliser les informations fournies par un utilisateur et interceptées par le composant, par exemple par des techniques classiques de « reniflage » de données (ou « data sniffing » selon la terminologie anglaise), pour effectuer des transactions de paiement frauduleuses.

De nombreuses techniques de l'art antérieur visent à protéger des terminaux de paiement de telles attaques.

Certaines techniques visent à lutter contre le vol de terminaux.

Il peut s'agir de moyens de protection physique, comme par exemple la solidarisation des terminaux sur un support, comme une base, un mur ou une tablette, de façon à les rendre difficilement transportables.

Cependant, pour des raisons de facilité d'utilisation, les terminaux de paiement sont souvent mobiles. C'est le cas par exemple dans des restaurants pour éviter à un client de se déplacer au moment de son paiement par carte bancaire. La faible taille et l'autonomie de tels terminaux rendent difficile leur surveillance (par des moyens humains par exemple, ou des moyens de vidéo surveillance). Un inconvénient de ces terminaux mobiles est qu'ils sont ainsi fortement exposés au vol.

D'autres solutions de l'art antérieur cherchent à prémunir les terminaux de paiement d'une intrusion. Il peut s'agir de moyens logiciel ou matériel, permettant notamment la détection d'une intrusion (par exemple une ouverture du boîtier d'un terminal).

Des moyens logiques de protection, comme l'implémentation de contremesures dans un microprocesseur d'un terminal de paiement, ont également été mis en œuvre.

Un inconvénient de ces techniques de l'art antérieur réside dans le fait que de telles techniques ne sont pas toujours suffisantes pour détecter une tentative de vol ou de détournement d'un terminal électronique ou parfois ne les détectent que tardivement, un moment après l'attaque.

3. Objectifs de l'invention

L'invention a notamment pour objectif de pallier ces inconvénients de l'art antérieur.

Plus précisément, un objectif de l'invention, dans au moins un de ses modes de réalisation, est de fournir un terminal électronique plus robuste aux attaques, et permettant notamment de détecter un vol ou une tentative de détournement du terminal de façon plus fiable par la mise en évidence de symptômes encore inconnus.

Un autre objectif de l'invention est, selon au moins un mode de réalisation, de proposer une solution discrète, non décelable par le tiers responsable de l'attaque du terminal, de façon notamment à aider les services de surveillance et/ou les forces de l'ordre à le confondre.

Un autre objectif de l'invention est, selon au moins un mode de réalisation, d'offrir une solution permettant une détection immédiate de l'attaque.

Un autre objectif de l'invention est, selon au moins un mode de réalisation, d'offrir une solution facile à implémenter aux fabricants de système de paiement.

4. Exposé de l'invention

Les inventeurs ont remarqué qu'une tentative d'attaque d'un terminal électronique pouvait être décelée par le caractère inhabituel d'une manipulation effectuée sur le terminal.

En effet, les terminaux destinés à manipuler des données sensibles (terminaux de paiement, terminaux de lecture et/ou de mise à jour de cartes électroniques contenant des données médicales personnelles et/ou permettant la déclaration d'actes médicaux auprès d'un organisme de santé...) sont souvent installés dans des lieux fermés, comme des cabinets médicaux, des secrétariats, des magasins, des restaurants ou des agences bancaires, ayant des horaires d'ouverture prédéfinis (classiquement 7h-21h) ou des jours de fermeture définissables à l'avance (week-end, jours fériés, période de vacances ou de travaux). Aussi, ils ne sont normalement utilisables que pendant les périodes d'accessibilité de ces lieux fermés. En conséquence, une action sur le terminal dans une période de fermeture d'un magasin ou d'un secrétariat (par exemple au milieu de la nuit) peut donc être considérée comme suspecte.

De ce fait, l'invention concerne un procédé de protection d'un terminal électronique, comprenant les étapes suivantes :

- activation d'un état de surveillance dudit terminal ;
- dans ledit état de surveillance, détection d'une manipulation dudit terminal, générant le passage dudit terminal dans un état dit suspect, représentatif d'un risque de tentative d'utilisation frauduleuse dudit terminal ;
- dans ledit état suspect, déclenchement d'une réaction par ledit terminal.

Ainsi, le procédé de l'invention permet de détecter des tentatives d'utilisation frauduleuses qui n'auraient pas été détectées par les solutions de l'art antérieur (détection d'intrusion dans le terminal, détection d'ouverture du terminal, substitution du terminal...), par exemple parce qu'il s'agit d'une manipulation discrète, classique pour un terminal de paiement mais inhabituelle pour le terminal concerné, car en dehors de ses plages horaires habituelles d'utilisation ou car la manipulation entraine un mouvement non autorisé du terminal, ou non compatible avec son installation.

Il s'agit là d'un avantage majeur par rapport à l'art antérieur.

Selon une caractéristique particulière de l'invention, ladite étape d'activation est mise en œuvre lorsque la valeur courante d'au moins une information de caractérisation d'un contexte dudit terminal se situe dans une plage de valeurs prédéfinie de ladite information de caractérisation.

Un tel mode de réalisation offre l'avantage de ne guetter les manipulations effectuées sur le terminal que lorsqu'une telle surveillance est utile (c'est–à-dire susceptible de mener à la confirmation d'une tentative d'utilisation frauduleuse), de façon à économiser les ressources du terminal, et notamment, dans le cas d'une utilisation du procédé de l'invention pour un terminal portable, la batterie du terminal.

Dans certains modes de réalisation de l'invention, la mise en état de surveillance peut être effectuée de façon automatique par le terminal, notamment de façon périodique, par exemple à l'heure de fermeture du magasin, du secrétariat ou de l'agence bancaire où se situe le terminal.

Dans ce mode de réalisation de l'invention, l'information de caractérisation est une information de type horodatage, permettant de définir des plages horaires pendant lesquelles on souhaite détecter des manipulations du terminal, celui-ci étant sensé pendant ces plages horaires ne pas être manipulé.

Ces plages horaires peuvent en particulier tenir compte de jours de fermeture (week-ends, jours fériés, vacances....) ou au contraire de périodes

programmées de maintenance du terminal.

Selon une caractéristique particulière de l'invention, ladite étape de détection d'une manipulation dudit terminal comprend une sous-étape de comparaison de la valeur courante d'au moins une information de caractérisation d'un contexte dudit terminal avec une plage de valeurs prédéfinie de ladite information de caractérisation.

Un tel mode de réalisation offre l'avantage de détecter systématiquement certaines manipulations, pour ensuite décider de leur caractère inhabituel ou non en fonction de certains paramètres prédéfinis (par exemple, dans le cas d'un terminal continuellement fixé sur un support, en comparant l'orientation ou la localisation du terminal, lors d'un mouvement du terminal, avec un plage de valeur prédéfinies, correspondant au degré de liberté du terminal sur un support).

Selon une caractéristique particulière de l'invention, ladite manipulation appartient au groupe d'événements comprenant :

- une action sur un composant de contrôle d'entrée d'une interface dudit terminal ;
- un retournement dudit terminal ;
- une rotation partielle dudit terminal ;
- un déplacement dudit terminal ;
- une pression sur une portion d'un boîtier du terminal;
- une combinaison d'au moins deux desdits évènements.

Par exemple, l'invention, selon ses différents modes de réalisation particuliers, permet de détecter une tentative d'utilisation frauduleuse par la détection d'un appui sur une touche du clavier du terminal, ou bien de la simple prise en main du terminal, exerçant une pression sur le boitier, ou bien une manipulation plus franche du terminal par un déplacement, retournement ou rotation de celui-ci ... Selon certains modes de réalisation, l'invention permet de détecter une tentative d'utilisation frauduleuse du terminal uniquement lorsqu'un ou plusieurs des événements précités se produisent (par exemple un

retournement du terminal et une pression sur le boitier).

Selon une caractéristique particulière de l'invention, ladite information de caractérisation appartient au groupe comprenant :

- une information issue d'un horodatage ;
- une orientation dudit terminal ;
- une localisation dudit terminal ;
- une accélération ou une vitesse de déplacement dudit terminal ;
- une combinaison d'au moins deux des informations du groupe.

Selon une caractéristique particulière de l'invention, le procédé comprend en outre une étape de désactivation dudit état de surveillance.

Ainsi, la surveillance du terminal peut être désactivée automatiquement, par exemple parce que l'information de caractérisation du contexte ne se situe plus dans la plage de valeurs prédéfinies, ou par un tiers autorisé (soit localement par le biais des moyens de contrôle d'interface du composant, soit à distance, par le biais de moyens de communication du terminal, par exemple une prise de contrôle à distance ou la réception d'un code particulier).

Selon une caractéristique particulière de l'invention, ladite étape de réaction dudit terminal comprend la mise en œuvre d'au moins une action appartenant au groupe comprenant :

- un blocage au moins partiel dudit terminal ;
- un effacement d'au moins une partie des données sensibles dudit terminal ;
- une falsification et/ou une corruption d'au moins une partie des données sensibles dudit terminal ;
- une émission d'un message d'alerte ;
- un enregistrement par ledit terminal d'au moins une information représentative de ladite manipulation ;
- une combinaison d'au moins deux desdits actions dudit groupe.

En particulier, un mode de réalisation dans lequel la réaction du terminal comprend la génération de données falsifiées offre l'avantage d'une discrétion

vis-à-vis d'un tiers malintentionné permettant d'éviter de l'alerter sur la mise en évidence de la tentative d'utilisation frauduleuse.

En particulier, il peut s'agir de remplacer les données sensibles par des données particulières, rendant évidente la falsification à un tiers de contrôle, et permettant ainsi d'améliorer la traçabilité des opérations effectuées par le tiers malintentionné après l'attaque.

Par ailleurs, l'émission d'un message d'alerte peut également être effectuée de manière discrète, sans attirer l'attention du tiers malintentionné, tout en permettant une intervention ultérieure, par exemple du propriétaire du terminal ou d'un service de surveillance...

Selon un mode de réalisation particulier de l'invention, ladite étape de réaction dudit terminal comprend en outre une étape d'actualisation d'un niveau d'alerte et ladite action est fonction dudit niveau d'alerte.

Un tel mode de réalisation offre en particulier l'avantage de permettre une réaction progressive du terminal aux manipulations détectées.

Par exemple, dans un premier niveau d'alerte, le terminal peut se contenter d'émettre un message vers un centre de surveillance. Dans un second niveau d'alerte, il peut en plus falsifier une partie des données sensibles qu'il contient.

Selon un autre aspect, l'invention concerne un produit programme d'ordinateur comprenant des instructions de code de programme pour la mise en œuvre du procédé précité (dans l'un quelconque de ses différents modes de réalisation), lorsque ledit programme est exécuté sur un ordinateur.

Dans un autre mode de réalisation de l'invention, il est proposé un médium de stockage lisible par ordinateur et non transitoire, stockant un programme d'ordinateur comprenant un jeu d'instructions exécutables par un ordinateur pour mettre en œuvre le procédé précité (dans l'un quelconque de ses différents modes de réalisation).

Selon encore un autre aspect, l'invention concerne aussi un terminal électronique comprenant :

- des moyens d'activation d'un état de surveillance dudit terminal;
- dans ledit état de surveillance, des moyens de détection d'une manipulation dudit terminal, générant le passage dudit terminal dans un état dit suspect, représentatif d'un risque de tentative d'utilisation frauduleuse dudit terminal ;
- dans ledit état suspect, des moyens de déclenchement d'une réaction par ledit terminal.

Selon une caractéristique particulière de l'invention, le terminal électronique consiste en un terminal de paiement.

5. Liste des 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 fonctionnel de l'invention dans un mode de réalisation ;
- la figure 2 illustre le fonctionnement dynamique du principe de l'invention, basé sur le synoptique statique de la figure 1 ;
- la figure 3 illustre le fonctionnement dynamique d'un premier mode de réalisation particulier de l'invention ;
- la figure 4 illustre le fonctionnement dynamique d'un second mode de réalisation particulier de l'invention ;
- la figure 5 illustre la structure d'un terminal selon l'invention.

Dans l'ensemble des figures ci-dessus, la même référence numérique est attribuée aux étapes ou composants similaires.

6. Description d'un mode de réalisation de l'invention

6.1 Principe général

Le principe général de l'invention consiste à détecter toute manipulation anormale d'un terminal électronique destiné à manipuler des données sensibles, par exemple un terminal de paiement, ou un terminal de

lecture et/ou de mise à jour de cartes électroniques contenant des données médicales personnelles et/ou de déclaration d'actes médicaux auprès d'un organisme de santé. A la différence des solutions de l'art antérieur, il peut s'agir d'une manipulation dont la nature en elle-même n'est pas caractéristique d'une attaque (par exemple parce qu'il s'agit d'une manipulation couramment effectuée sur le terminal) mais est considérée comme suspecte en fonction du contexte particulier d'utilisation propre au terminal.

6.2 Description du synoptique fonctionnel de l'invention

On considère par la suite un exemple de mise en œuvre de l'invention pour un terminal de paiement.

On présente, en relation avec la figure 1, un mode particulier de mise en œuvre du procédé selon l'invention.

Dans ce mode particulier de réalisation de l'invention, un terminal de paiement 100 permet à un utilisateur d'effectuer des règlements et transmet des informations relatives à ces règlements vers un système de gestion distant 160, par exemple un système de gestion de terminaux (ou TMS, pour « Terminal Management System » selon la terminologie anglaise).

Un tel terminal est muni de composants de contrôle d'interface, permettant un échange d'informations avec un utilisateur du terminal. Il comprend par exemple un écran 110 pour la restitution d'informations ou l'interrogation d'un utilisateur, et un clavier 120, permettant la saisie de données par un utilisateur. Il peut s'agir d'un clavier matériel 120 (comme représenté en figure 1) ou d'un clavier virtuel, apparaissant par exemple sur l'écran 110.

Selon l'invention, le terminal comprend également des moyens de détermination (130, 140) de la valeur d'une information de caractérisation d'un contexte du terminal, par exemple par le biais de composants électroniques implantés sur la carte mère du terminal 100.

En particulier, dans le mode de réalisation présenté en figure 1, le terminal peut comprendre des moyens de détermination 130 d'une heure

courante, par exemple une horloge. Il peut également être muni de moyens de synchronisation de cette horloge avec au moins un référentiel temporel.

Dans le mode particulier illustré en figure 1, le terminal comprend de plus des moyens de détermination 140 d'une position ou d'une variation de position du terminal. Il peut par exemple s'agir de moyens de localisation du terminal, par exemple par GPS, et/ou de moyens de détermination d'un déplacement ou d'une orientation du terminal. Il peut ainsi s'agir d'au moins un accéléromètre, pour la mesure d'accélérations linéaires, et/ou d'au moins un gyromètre, pour la mesure de vitesses angulaires, et/ou d'au moins une centrale inertielle (ou IRS, pour Inertial Reference System, selon la terminologie anglaise), pour mesurer à la fois plusieurs accélérations et/ou vitesses angulaires ou encore d'au moins un inclinomètre, pour mesurer une orientation du terminal.

Ainsi, selon le mode particulier de réalisation illustré en figure 1, le terminal comprend une centrale inertielle 140.

Dans certains modes de réalisation particuliers où le rendu des informations visualisées sur l'écran 110 du terminal 100 est influencé par un mouvement ou une orientation du terminal 100, une même centrale inertielle peut être utilisée à la fois pour la définition du rendu des informations sur l'écran et pour la mise en œuvre du procédé de l'invention. Dans d'autres modes de réalisation, le terminal peut comprendre plusieurs centrales inertielles, certaines étant dédiées à la définition d'un rendu et d'autres au procédé de l'invention.

Dans d'autres modes de réalisation, éventuellement complémentaire, le terminal peut comprendre d'autres moyens de détection d'une manipulation du terminal, par exemple des moyens de détection d'une pression appliquée sur une portion du terminal .

6.3 Description du fonctionnement dynamique de l'invention

On présente en liaison avec la figure 2 le principe de fonctionnement dynamique de l'invention dans un mode particulier de réalisation, compatible avec le terminal objet de la figure 1.

Le procédé de l'invention comprend ainsi une étape 200 d'activation de l'état de surveillance du terminal.

Lorsque le terminal est en état de surveillance, le procédé comprend ensuite une étape de détection 210 d'une manipulation effectuée sur le terminal. Selon les modes de réalisation de l'invention, il peut s'agir d'une manipulation particulière détectée par un moyen de détection particulier (par exemple une centrale inertielle dans le cas d'un déplacement, d'un retournement ou d'une rotation partielle du terminal) ou de toute manipulation détectée par l'un quelconque des moyens de détection d'une manipulation du terminal.

Par exemple, il peut s'agir de la simple utilisation d'un composant d'interface du terminal ou d'une pression appliquée sur une paroi du boîtier du terminal, par exemple lors de la prise en main du terminal.

La détection d'une telle manipulation génère le passage 220 du terminal dans un état dit suspect, représentatif d'un risque de tentative d'utilisation frauduleuse du terminal et est suivie par une étape de déclenchement 230 d'une réaction du terminal.

Dans certains modes de réalisation de l'invention, cette réaction peut être locale. Il peut s'agir par exemple d'un blocage au moins partiel du terminal, et/ou d'un effacement et/ou d'une falsification et/ou d'une corruption d'au moins une partie des données sensibles du terminal, et/ou de l'enregistrement d'informations représentatives de la manipulation (notamment la date, l'heure, la nature de la manipulation et/ou d'une identification d'au moins un moyen de détection ayant permis la détection).

Dans d'autres modes de réalisation, éventuellement complémentaires, l'étape de réaction peut mettre en œuvre des moyens de communication vers un tiers habilité, comme un propriétaire du terminal, un centre de télésurveillance d'un service de police ou d'une société privée, ou encore un service opérationnel distant dans le cadre d'un système de gestion de terminaux (ou TMS, pour « Terminal Management System » selon la terminologie anglaise).

Il peut s'agir notamment d'un appel audio, lorsque le terminal possède des moyens de synthèse vocal par exemple ou de la génération d'un message textuel, de type SMS ou email par exemple, ou encore, lorsque le terminal possède des moyens d'acquisition d'images ou de vidéo, de l'émission d'un flux multimédia relatif à l'instant de la manipulation, permettant au tiers habilité de vérifier facilement si une tentative d'atteinte au terminal a réellement lieu ou s'il s'agit d'une fausse alarme (par exemple, une manipulation attribuable à un animal ou à une chute d'un objet). Un tel flux multimédia peut de plus aider à déterminer l'identité des tiers malintentionnés.

Dans une variante, les actions effectuées localement par le terminal peuvent en particulier être commandées à distance par le tiers habilité.

Dans certains modes de réalisation, la réaction 230 du terminal peut également inclure une étape d'actualisation d'un niveau d'alerte et l'action du terminal, suite à la manipulation détectée, peut être fonction du niveau d'alerte.

Par exemple, lors de l'activation de la surveillance du terminal, le niveau d'alerte du terminal peut être fixé à sa valeur minimale (valeur « 0 » par exemple) et chaque manipulation peut provoquer l'incrémentation du niveau d'alerte. A une première valeur (« 1 » par exemple), peut correspondre un enregistrement local au terminal d'informations représentatives de la manipulation, à un second niveau d'alerte (valeur « 2 » par exemple), peut correspondre l'émission d'une alarme (audio, textuelle ou visuelle) vers un tiers habilité, à un troisième niveau d'alerte peut correspondre une falsification ou une corruption des données sensibles. Un tel mode de réaction permet de disposer d'une réponse proportionnelle à la probabilité de la menace, de façon à ne pas nuire au fonctionnement opérationnel du terminal pour une fausse alarme par exemple.

Le procédé peut également comprendre une étape de remise à sa valeur minimale du niveau d'alerte, suite à une décision du tiers habilité (concluant à une fausse alarme par exemple).

Dans certains modes de réalisation, le procédé peut comprendre en

outre une étape de désactivation de l'état de surveillance du terminal. Cette étape peut notamment être mise en œuvre lors d'une opération de maintenance du terminal.

6.4 Description d'un premier mode de réalisation particulier de l'invention

On présente en liaison avec la figure 3 un premier mode de réalisation particulier de l'invention, adapté par exemple à une surveillance d'un terminal de paiement portatif, placé dans un restaurant.

Dans ce mode de réalisation particulier, l'étape d'activation 200 de la surveillance du terminal est mise en œuvre automatiquement par le terminal, lorsque la valeur courante d'au moins une information de caractérisation du contexte du terminal (par exemple l'heure courante) se situe dans une plage de valeurs prédéfinie (par exemple une tranche horaire de fermeture du restaurant).

Le procédé comprend ainsi une étape de détermination 300 de la valeur courante de l'information de caractérisation, puis une étape de comparaison 310 de cette valeur courante avec une plage de valeurs prédéfinie. Cette plage de valeur peut notamment avoir être définie par un paramétrage du terminal, réalisé localement par un opérateur (le restaurateur ou l'installateur du terminal) à l'aide des composants de contrôle d'interface du terminal, ou effectué à distance depuis un serveur dédié au management du parc de terminaux auquel appartient le terminal. Ce paramétrage peut notamment tenir compte du fuseau horaire dans lequel se situe le terminal, des jours de fermeture de l'établissement (week-ends, jours fériés ou vacances) ou de maintenance du terminal. Il peut également être effectué automatiquement, grâce à une synchronisation avec des données contenues dans un agenda et/ou un calendrier électroniques, stockés localement sur le terminal ou sur un serveur distant.

En outre, le procédé peut en particulier comprendre une étape de désactivation de l'état de surveillance du terminal, par exemple lorsque

l'information de caractérisation du contexte du terminal se situe à nouveau dans la plage de valeurs prédéfinie.

L'invention permet ainsi une protection automatique du terminal, sans action journalière d'un opérateur, activée uniquement lors des plages de fermeture du lieu où se situe le terminal.

Dans le premier mode de réalisation particulier illustré en figure 3, on retrouve ensuite les étapes 210, 220 et 230, commentées en liaison avec la figure 2.

6.5 Description d'un second mode de réalisation particulier de l'invention

On présente en liaison avec la figure 4 un second mode de réalisation particulier de l'invention, adapté par exemple à une surveillance d'un terminal électronique assujetti à un support, de façon fixe ou de manière à limiter ses déplacements, par exemple par le biais d'une liaison filaire. Un tel terminal peut par exemple être situé dans un magasin.

Dans ce cas particulier, après activation 200 de l'état de surveillance, l'étape de détection 210 d'une manipulation comprend une sous-étape de détermination 410 de la valeur courante d'une information de caractérisation d'un contexte du terminal et une sous-étape de comparaison 420 de cette valeur courante avec une plage de valeurs prédéfinie. Cette sous-étape de détermination 410 peut notamment faire suite à toute manipulation détectée 400.

Dans le mode de réalisation illustré, il peut par exemple s'agir d'une information de caractérisation liée à une position et/ ou à un mouvement (déplacement, rotation, accélération) du terminal. En effet, tout mouvement du terminal, impossible en pratique du fait de la liaison du terminal avec son support, pourra être considéré comme suspect, qu'il survienne pendant les heures d'ouverture ou de fermeture du magasin. Il pourrait par exemple s'agir d'une tentative de retournement du terminal, pour le remplacer par un terminal corrompu, ou d'une tentative de vol du terminal.

Dans le second mode de réalisation particulier illustré en figure 4, on retrouve ensuite les étapes 220 et 230 commentées en liaison avec la figure 2.

6.6 Description d'autres modes de réalisation particuliers de l'invention

Les deux modes de réalisation présentés ci-dessus peuvent bien sûr être combinés et mettre en œuvre des informations de caractérisation différentes.

Par exemple, dans un mode de réalisation particulier, l'activation de l'état de surveillance du terminal sera effectuée automatiquement par comparaison de l'heure et de la date courante avec une plage de valeurs horodatées prédéfinie et l'étape de détection 210 d'une manipulation comprendra la détermination d'une orientation du terminal et sa comparaison avec une plage angulaire prédéfinie, ou la détermination d'une localisation courante du terminal et sa comparaison avec une zone géographique prédéterminée ou encore la détermination d'une accélération courante du terminal et sa comparaison avec une valeur maximale prédéfinie, la détection d'une forte accélération, non compatible avec une utilisation courante, pouvant traduire l'occurrence d'un vol à l'arraché.

De tels modes de réalisation sont par exemple également adaptés à la surveillance d'un terminal portatif fixé sur un support pendant les heures de fermeture d'un restaurant ou d'un secrétariat, afin notamment de recharger la batterie du terminal. Ils permettent notamment de réagir systématiquement à tout mouvement du terminal mais seulement pendant les heures de fermeture du restaurant ou du secrétariat.

6.7 Structure d'un terminal électronique selon l'invention

On présente, en relation avec la figure 5, la structure simplifiée d'un terminal électronique selon l'invention.

En sus des éléments fonctionnels détaillés en figure 1, un tel terminal comprend une mémoire 500 comprenant une mémoire tampon, une unité de traitement 510, équipée par exemple d'un microprocesseur µP, et pilotée par un

programme d'ordinateur 520, dont l'exécution met en œuvre un procédé de protection, selon l'un des modes de réalisation particuliers de l'invention.

A l'initialisation, les instructions de code du programme d'ordinateur 520 sont par exemple chargées dans une mémoire RAM avant d'être exécutées par le processeur de l'unité de traitement 510.

L'unité de traitement 510 reçoit en entrée un entête d'un flux de données.

Le microprocesseur de l'unité de traitement 510 met en œuvre les étapes du procédé de protection décrit précédemment, selon les instructions du programme d'ordinateur 520.

A cette fin, le terminal électronique comprend, outre la mémoire tampon 500 :

- des moyens d'activation d'un état de surveillance du terminal;
- dans l'état de surveillance, des moyens de détection d'une manipulation du terminal, générant le passage du terminal dans un état dit suspect, représentatif d'un risque de tentative d'utilisation frauduleuse du terminal ;
- dans ledit état suspect, des moyens de déclenchement d'une réaction par le terminal.

Ces moyens sont pilotés par le microprocesseur de l'unité de traitement 510.

Selon un mode de réalisation, l'invention est mise en œuvre au moyen de composants logiciels et/ou matériels. Dans cette optique, le terme "moyens" peut correspondre dans ce document aussi bien à un composant logiciel, qu'à un composant matériel ou à un ensemble de composants matériels et logiciels.

Un composant logiciel correspond à un ou plusieurs programmes d'ordinateur, un ou plusieurs sous-programmes d'un programme, ou de manière plus générale à tout élément d'un programme ou d'un logiciel apte à mettre en œuvre une fonction ou un ensemble de fonctions, selon ce qui est décrit ci-dessous pour les moyens concernés. Un tel composant logiciel est exécuté par

un processeur de données d'une entité physique (terminal, serveur, passerelle, set-top-box, routeur, etc...) et est susceptible d'accéder aux ressources matérielles de cette entité physique (mémoires, supports d'enregistrement, bus de communication, cartes électroniques d'entrées/sorties, interfaces utilisateur, etc...).

De la même manière, un composant matériel correspond à tout élément d'un ensemble matériel (ou hardware) apte à mettre en œuvre une fonction ou un ensemble de fonctions, selon ce qui est décrit ci-dessous pour le module concerné. Il peut s'agir d'un composant matériel programmable ou avec processeur intégré pour l'exécution de logiciel, par exemple un circuit intégré, une carte à puce, une carte à mémoire, une carte électronique pour l'exécution d'un micrologiciel (firmware), etc.

Le terminal selon l'invention peut en particulier comprendre les composants logiciels ou matériels illustrés en figure 1.

REVENDICATIONS

1. Procédé de protection d'un terminal électronique comprenant les étapes suivantes :

- activation d'un état de surveillance dudit terminal ;
- dans ledit état de surveillance, détection d'une manipulation dudit terminal, générant le passage dudit terminal dans un état dit suspect, représentatif d'un risque de tentative d'utilisation frauduleuse dudit terminal ;
- dans ledit état suspect, déclenchement d'une réaction par ledit terminal ;

caractérisé en ce que ladite étape de réaction dudit terminal comprend une étape d'actualisation d'un niveau d'alerte, représentatif d'une probabilité de tentative d'utilisation frauduleuse dudit terminal, et une étape de mise en œuvre d'au moins une action réactive fonction dudit niveau d'alerte.

2. Procédé de protection d'un terminal électronique selon la revendication 1 caractérisé en ce que ladite étape d'activation est mise en œuvre lorsque la valeur courante d'au moins une information de caractérisation d'un contexte dudit terminal se situe dans une plage de valeurs prédéfinie de ladite information de caractérisation.

3. Procédé de protection d'un terminal électronique selon la revendication 1 ou 2 caractérisé en ce que ladite étape de détection d'une manipulation dudit terminal comprend une sous-étape de comparaison de la valeur courante d'au moins une information de caractérisation d'un contexte dudit terminal avec une plage de valeurs prédéfinie de ladite information de caractérisation.

4. Procédé de protection d'un terminal électronique, selon l'une quelconque des revendications 1 à 3, caractérisé en ce que ladite manipulation appartient au groupe d'événements comprenant :

- une action sur un composant de contrôle d'entrée d'une interface dudit

terminal ;

- un retournement dudit terminal ;
- une rotation partielle dudit terminal ;
- un déplacement dudit terminal ;
- une pression sur une portion d'un boîtier du terminal;
- une combinaison d'au moins deux desdits évènements.

5. Procédé de protection d'un terminal électronique, selon l'une quelconque des revendications 1 à 4, caractérisé en ce que ladite information de caractérisation appartient au groupe comprenant :

- une information issue d'un horodatage ;
- une orientation dudit terminal ;
- une localisation dudit terminal ;
- une accélération ou une vitesse de déplacement dudit terminal ;
- une combinaison d'au moins deux des informations du groupe.

6. Procédé de protection d'un terminal électronique, selon l'une quelconque des revendications 1 à 5, caractérisé en ce que le procédé comprend en outre une étape de désactivation dudit état de surveillance.

7. Procédé de protection d'un terminal électronique, selon l'une quelconque des revendications 1 à 6, caractérisé en ce que ladite action réactive appartient au groupe comprenant :

- un blocage au moins partiel dudit terminal ;
- un effacement d'au moins une partie des données sensibles dudit terminal ;
- une falsification et/ou une corruption d'au moins une partie des données sensibles dudit terminal ;
- une émission d'un message d'alerte ;
- un enregistrement par ledit terminal d'au moins une information représentative de ladite manipulation ;
- une combinaison d'au moins deux desdits actions dudit groupe.

8. Produit programme d'ordinateur, comprenant des instructions de code de programme pour la mise en œuvre du procédé de protection selon au moins une des revendications 1 à 7, lorsque ledit programme est exécuté sur un ordinateur.

9. Terminal électronique comprenant :

- des moyens d'activation d'un état de surveillance dudit terminal;
- dans ledit état de surveillance, des moyens de détection d'une manipulation dudit terminal, générant le passage dudit terminal dans un état dit suspect, représentatif d'un risque de tentative d'utilisation frauduleuse dudit terminal ;
- dans ledit état suspect, des moyens de déclenchement d'une réaction par ledit terminal ;

caractérisé en ce que lesdits moyens de déclenchement d'une réaction par ledit terminal comprennent des moyens d'actualisation d'un niveau d'alerte représentatif d'une probabilité de tentative d'utilisation frauduleuse dudit terminal, et des moyens de mise en œuvre d'au moins une action réactive fonction dudit niveau d'alerte.

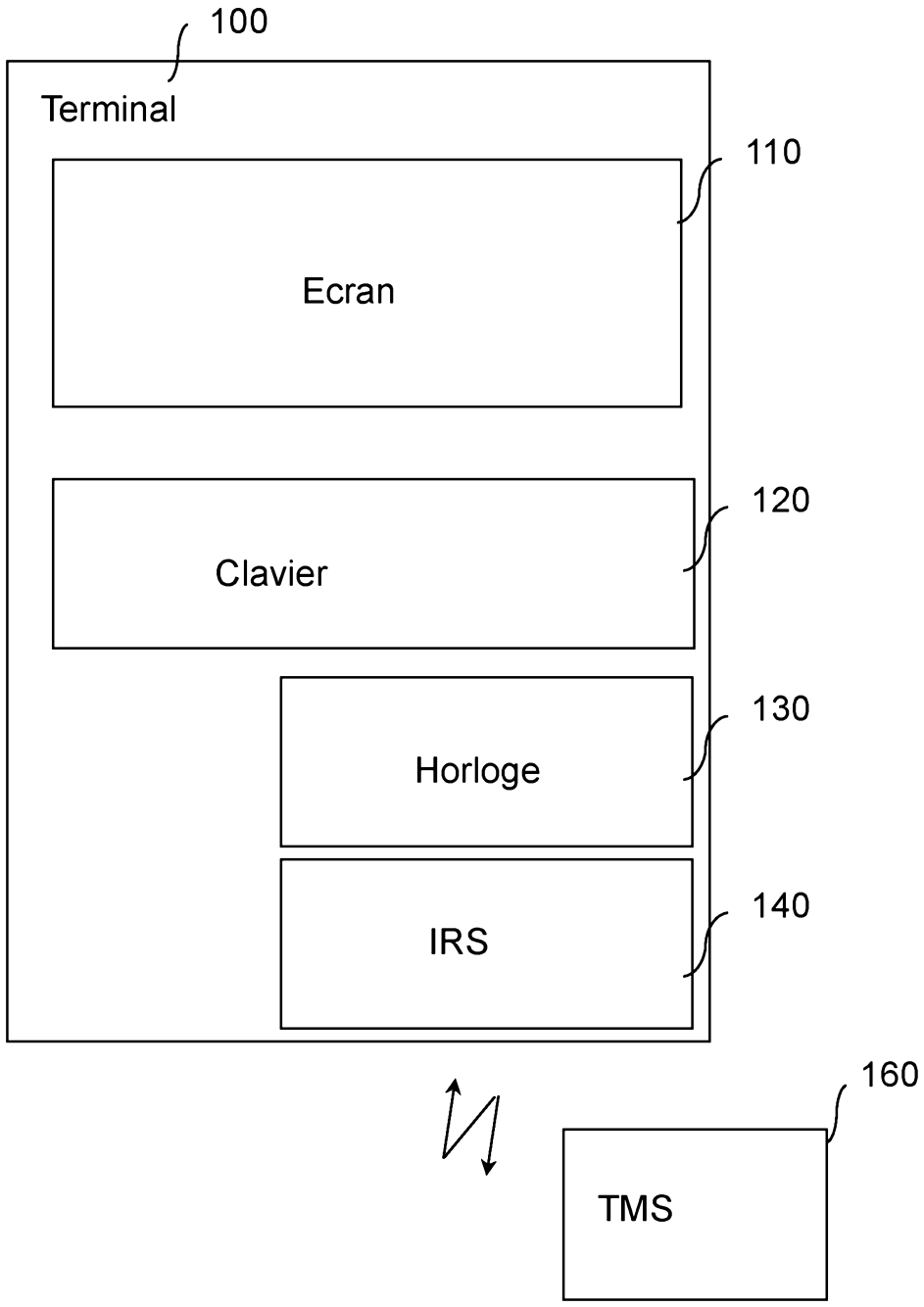
100
Terminal
110
Ecran
120
Clavier
130
Horloge
140
IRS
160
TMS

Figure 1

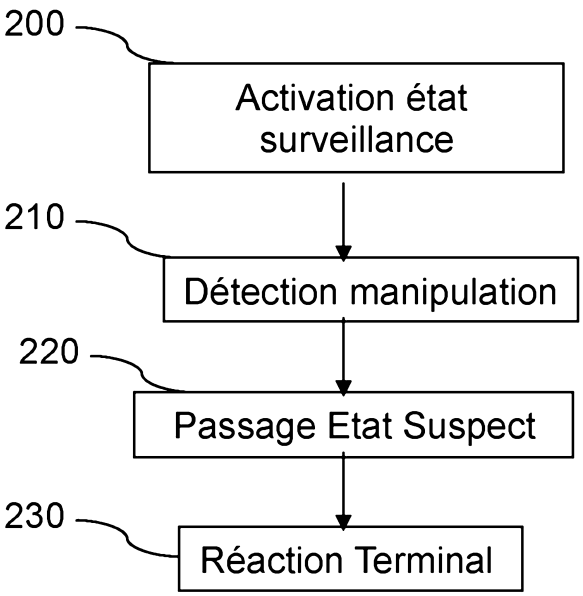
200
Activation état surveillance
210
Détection manipulation
220
Passage Etat Suspect
230
Réaction Terminal

Figure 2

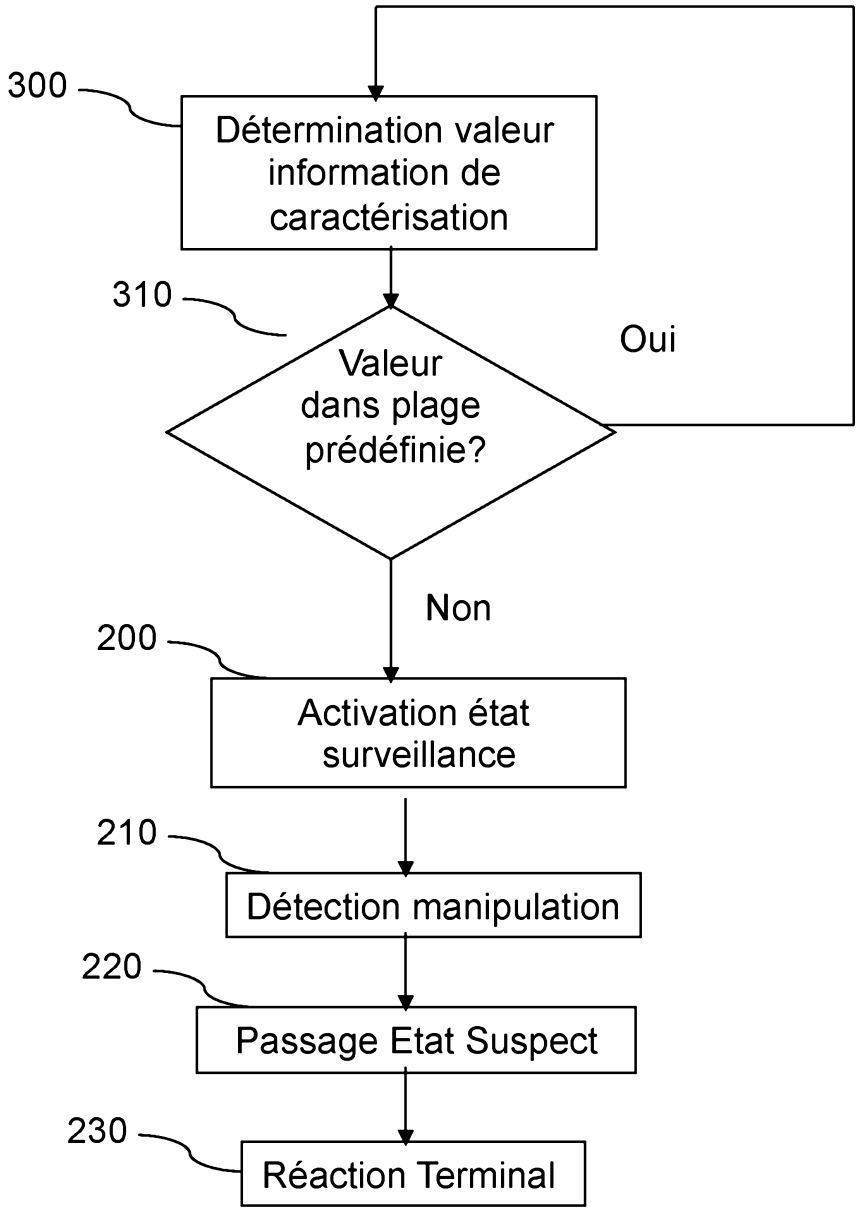
300
Détermination valeur information de caractérisation
310
Valeur dans plage prédéfinie?
Oui
Non
200
Activation état surveillance
210
Détection manipulation
220
Passage Etat Suspect
230
Réaction Terminal

Figure 3

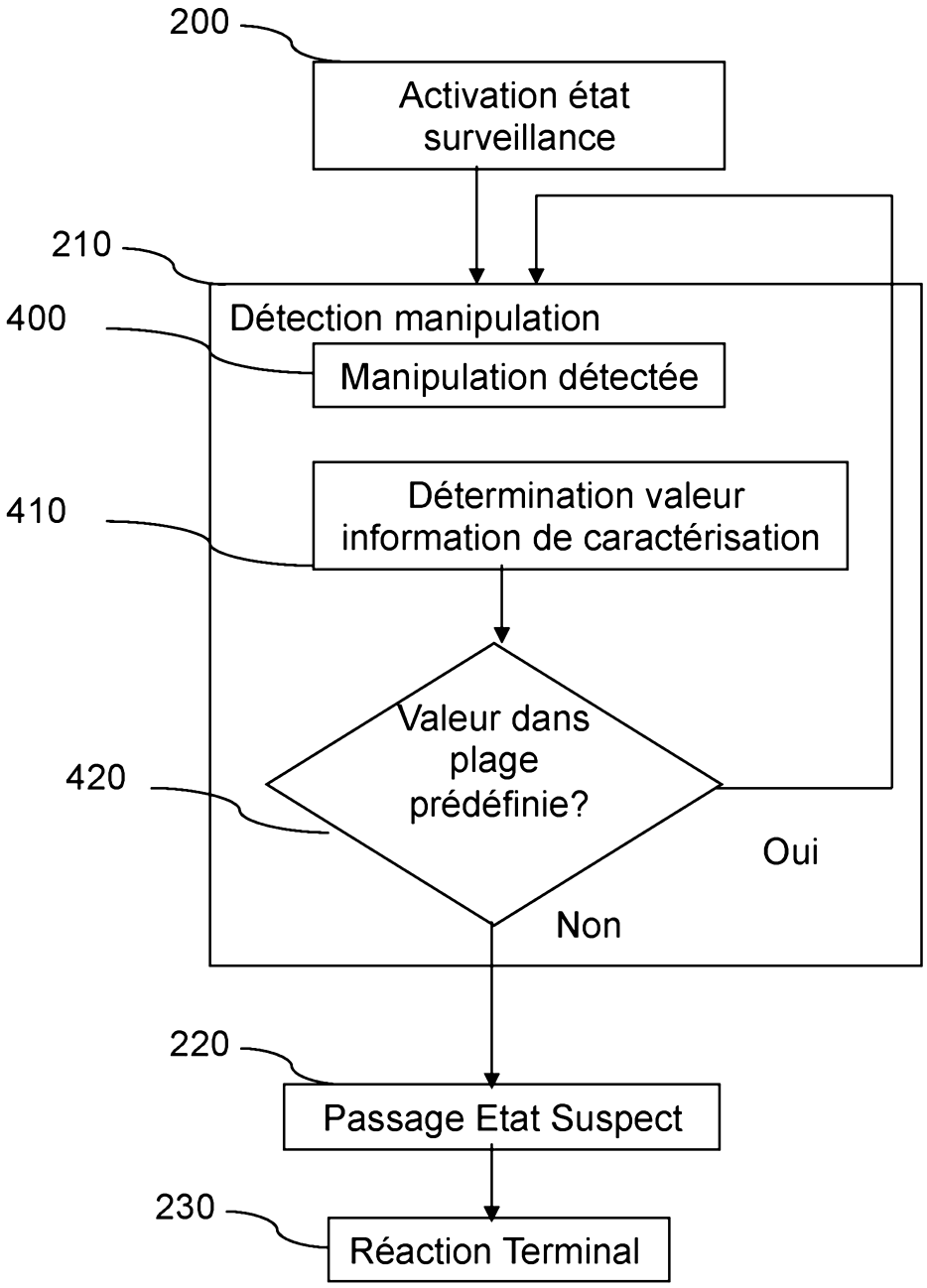
200
Activation état surveillance
210
Détection manipulation
400
Manipulation détectée
410
Détermination valeur information de caractérisation
420
Valeur dans plage prédéfinie?
Oui
Non
220
Passage Etat Suspect
230
Réaction Terminal

Figure 4

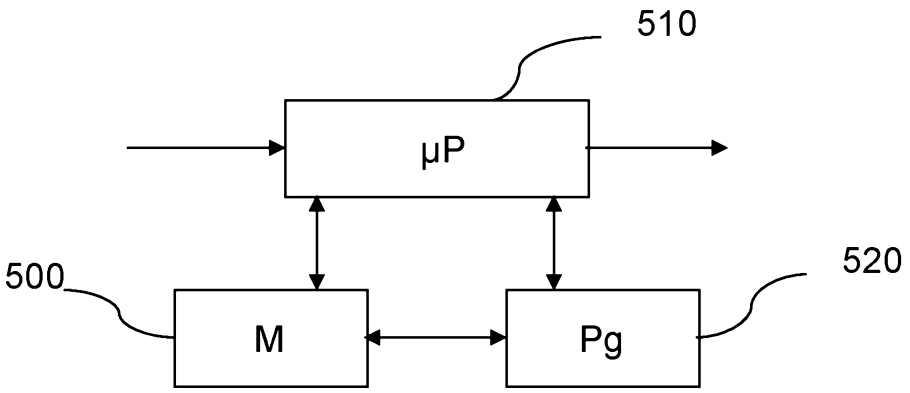

Figure 5

N° d'enregistrement national : 1262038 N° de publication : 2999751

RAPPORT DE RECHERCHE

articles L.612-14, L.612-17 et R.612-53 à 69 du code de la propriété intellectuelle

OBJET DU RAPPORT DE RECHERCHE

L'I.N.P.I. annexe à chaque brevet un "RAPPORT DE RECHERCHE" citant les éléments de l'état de la technique qui peuvent être pris en considération pour apprécier la brevetabilité de l'invention, au sens des articles L. 611-11 (nouveauté) et L. 611-14 (activité inventive) du code de la propriété intellectuelle. Ce rapport porte sur les revendications du brevet qui définissent l'objet de l'invention et délimitent l'étendue de la protection.

Après délivrance, l'I.N.P.I. peut, à la requête de toute personne intéressée, formuler un "AVIS DOCUMENTAIRE" sur la base des documents cités dans ce rapport de recherche et de tout autre document que le requérant souhaite voir prendre en considération.

CONDITIONS D'ÉTABLISSEMENT DU PRÉSENT RAPPORT DE RECHERCHE

- [x] Le demandeur a présenté des observations en réponse au rapport de recherche préliminaire.
- [ ] Le demandeur a maintenu les revendications.
- [x] Le demandeur a modifié les revendications.
- [ ] Le demandeur a modifié la description pour en éliminer les éléments qui n'étaient plus en concordance avec les nouvelles revendications.
- [ ] Les tiers ont présenté des observations après publication du rapport de recherche préliminaire.
- [ ] Un rapport de recherche préliminaire complémentaire a été établi.

DOCUMENTS CITÉS DANS LE PRÉSENT RAPPORT DE RECHERCHE

La répartition des documents entre les rubriques 1, 2 et 3 tient compte, le cas échéant, des revendications déposées en dernier lieu et/ou des observations présentées.

- [x] Les documents énumérés à la rubrique 1 ci-après sont susceptibles d'être pris en considération pour apprécier la brevetabilité de l'invention.
- [ ] Les documents énumérés à la rubrique 2 ci-après illustrent l'arrière-plan technologique général.
- [ ] Les documents énumérés à la rubrique 3 ci-après ont été cités en cours de procédure, mais leur pertinence dépend de la validité des priorités revendiquées.
- [ ] Aucun document n'a été cité en cours de procédure.

N° d'enregistrement national : 1262038 N° de publication : 2999751

1. ELEMENTS DE L'ETAT DE LA TECHNIQUE SUSCEPTIBLES D'ETRE PRIS EN CONSIDERATION POUR APPRECIER LA BREVETABILITE DE L'INVENTION

US 2005/222801 A1 (WULFF THOMAS [US] ET AL)
6 octobre 2005 (2005-10-06)

2. ELEMENTS DE L'ETAT DE LA TECHNIQUE ILLUSTRANT L'ARRIERE-PLAN TECHNOLOGIQUE GENERAL

NEANT

3. ELEMENTS DE L'ETAT DE LA TECHNIQUE DONT LA PERTINENCE DEPEND DE LA VALIDITE DES PRIORITES

NEANT