

12

DEMANDE DE BREVET D'INVENTION

A1

22 Date de dépôt : 22.04.10.

30 Priorité :

43 Date de mise à la disposition du public de la
 demande : 28.10.11 Bulletin 11/43.

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 :

71 Demandeur(s) : STMICROELECTRONICS (ROUS-
 SET) SAS — FR.

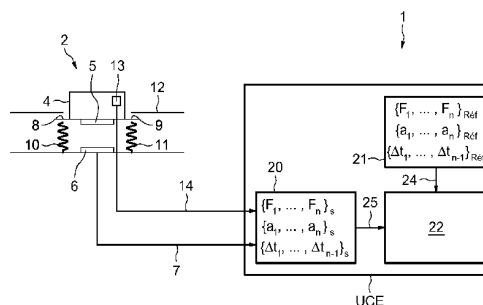
72 Inventeur(s) : TEGLIA YANNICK.

73 Titulaire(s) : STMICROELECTRONICS (ROUSSET)
 SAS.

74 Mandataire(s) : BUREAU D.A. CASALONGA &
 JOSSE.

54 PROCÉDE ET DISPOSITIF D'AUTHENTIFICATION D'UN UTILISATEUR A L'AIDE DE DONNEES
 BIOMETRIQUES.

57 Système d'authentification comprenant un dispositif
 de saisie (2) comportant une pluralité d'éléments de saisie
 (4) configurés pour saisir respectivement des caractères en
 réponse à une saisie d'une séquence d'au moins un caractè-
 re effectuée par un utilisateur, le dispositif de saisie (2)
 comprenant au moins un moyen de détermination (13), cou-
 plé à au moins un élément de saisie (4), pour déterminer
 une force exercée sur ledit au moins un élément de saisie
 (4), le système comprenant un moyen d'enregistrement (20)
 pour enregistrer une série d'au moins une force exercée sur
 ledit au moins un élément de saisie (4), une mémoire (21)
 configurée pour stocker une série d'au moins une force de
 référence, et des moyens de comparaison (22) configurés
 pour comparer la série d'au moins une force exercée avec
 la série d'au moins une force de référence.



DEMANDE DE BREVET

B09-4733FR

Société par actions simplifiée dite : **STMicroelectronics (ROUSSET) SAS**

Procédé et dispositif d'authentification d'un utilisateur à l'aide de données biométriques

Invention de : **Yannick TEGLIA**

Procédé et dispositif d'authentification d'un utilisateur à l'aide de données biométriques

5 L'invention concerne l'authentification d'un individu, et en particulier un système d'authentification biométrique.

En général, on identifie les individus par une authentification à l'aide d'un mot de passe.

10 En particulier, on identifie un individu dès qu'il souhaite accéder à des données confidentielles afin de garantir la sécurité de telles données. Les mots de passe ainsi utilisés font partie des connaissances de l'utilisateur.

On peut également améliorer la sécurité d'accès à ces données en utilisant un support externe à l'utilisateur, par exemple une carte à microprocesseur, notamment une carte bancaire, sur laquelle est stocké
15 le mot de passe de l'utilisateur et qui permet de vérifier ce que connaît l'utilisateur. Dans ce cas, l'utilisateur connaît son mot de passe, il le saisit sur un clavier numérique, par exemple un clavier d'un terminal d'ordinateur, et la carte à microprocesseur permet de comparer la séquence saisie par l'utilisateur avec le mot de passe crypté qui est
20 stocké sur la carte à microprocesseur.

L'inconvénient des mots de passe est qu'ils peuvent être volés, ou encore qu'une personne peut se substituer à celui qui détient le mot de passe. En outre, le support externe qui stocke le mot de passe crypté de l'utilisateur n'est pas non plus suffisant pour garantir l'accès
25 aux données confidentielles de l'utilisateur, puisque celui-ci peut également être volé et être utilisé frauduleusement.

Un autre inconvénient est qu'une autre personne peut se substituer à l'utilisateur en connaissant le mot de passe et en possédant la carte à microprocesseur de l'utilisateur, de manière
30 frauduleuse ou non. Cet inconvénient découle directement du fait que le mot de passe n'est pas lié intrinsèquement à l'individu, puisque plusieurs personnes peuvent être authentifiées avec un mot de passe unique.

Afin d'améliorer les systèmes d'authentification, on utilise actuellement des systèmes biométriques. Les données biométriques, sont des données intrinsèques à l'individu, et peuvent résoudre une partie de ces problèmes.

5 Il existe actuellement des reconnaissances rétinienne ou des reconnaissances d'empreintes digitales. Mais ces dispositifs sont complexes et nécessitent des algorithmes de traitement hautement élaborés afin de traiter la masse importante de données que peut fournir une rétine ou une empreinte digitale.

10 Par ailleurs, les empreintes digitales peuvent être reproduites. Un autre inconvénient de la reconnaissance par empreintes digitales est que l'extrémité des doigts peut être recouverte d'une légère couche de dépôt, telle qu'une couche de poussière ou de corps gras, qui peut perturber les systèmes de mesure.

15 Un autre inconvénient des systèmes biométriques actuels est que l'on pourrait forcer une personne à placer sa rétine, ou ses doigts, devant les systèmes d'authentification, et ainsi forcer les accès aux données de l'utilisateur.

20 Il est donc proposé, en particulier, de fournir un moyen pour identifier un individu, qui soit moins complexe que ceux cités précédemment et qui puisse améliorer la sécurité de l'accès aux données de l'utilisateur.

25 Selon un aspect, il est proposé un procédé d'authentification comprenant une détermination d'une séquence d'au moins un caractère saisie par un utilisateur sur un dispositif de saisie de caractères, une détermination d'une séquence d'au moins un caractère de référence et une comparaison de la séquence saisie avec la séquence de référence.

30 Selon cet aspect, la détermination de la séquence saisie comporte une détermination d'une série d'au moins une force exercée sur le dispositif de saisie lors de la saisie de la séquence, la détermination de la séquence de référence comporte une détermination d'une série d'au moins une force de référence associée à l'utilisateur, et ladite comparaison des séquences comporte une comparaison de la

série d'au moins une force exercée sur le dispositif de saisie avec la série d'au moins une force de référence.

Ainsi, on fournit un procédé d'authentification d'un individu basé sur des données biométriques telles que la gestuelle de l'individu.

5 En effet, chaque personne a une façon propre pour saisir un mot de passe sur un dispositif de saisie, à une tolérance d'erreur près. La détection des forces exercées sur le dispositif de saisie permet donc d'identifier la personne de manière efficace, tout en étant moins

10 complexe à mettre en œuvre par rapport aux procédés biométriques actuels. En outre, la prise en compte de la gestuelle d'un individu peut améliorer la reconnaissance d'un individu par rapport aux systèmes qui utilisent des données d'empreintes digitales ou de rétines. En particulier, un utilisateur mis en situation de stress (parce qu'il est par exemple contraint par une autre personne de taper son mot de passe)

15 ne produira pas les mêmes forces sur le dispositif de saisie que si celui-ci était en situation normale.

En outre, il est très difficile, voire quasiment impossible, de reproduire la gestuelle d'un individu par une tierce personne.

Il est également difficile d'imiter les caractéristiques

20 intrinsèques de la gestuelle d'un individu, telles que les forces exercées par l'individu, contrairement à ses empreintes digitales par exemple.

Ce procédé est donc plus simple que ceux qui consistent à détecter une empreinte rétinienne ou digitale, et permet de renforcer

25 l'identification de l'individu car un individu en situation de stress aura bien entendu la même rétine et la même empreinte digitale.

Selon un mode de mise en œuvre, la détermination de la séquence saisie comprend une détermination d'une série de plusieurs forces exercées successivement sur le dispositif de saisie, la

30 détermination de la séquence de référence comporte la détermination d'une succession de plusieurs forces de référence associées à l'utilisateur et ladite comparaison de séquences comporte une comparaison de ladite série de forces exercées sur le dispositif de saisie avec ladite succession de forces de référence.

Selon un autre mode de mise en œuvre, la détermination de la séquence saisie comprend la détermination d'une série de plusieurs forces exercées sur le dispositif de saisie selon plusieurs axes de direction, et la séquence de référence comporte une série de plusieurs forces de référence associées à ces axes de direction.

Ainsi, on fournit un moyen amélioré pour déterminer des forces exercées par l'utilisateur sur le dispositif de saisie. En effet, même si un seul axe de mesure est suffisant, on pourra utiliser les composantes de la force exercée sur le dispositif suivant trois axes différents de manière à préciser la comparaison de la force exercée par l'utilisateur et la force de référence.

Avantageusement, la détermination de la ou les forces exercées sur le dispositif de saisie, ainsi que la ou les forces de référence, comportent au moins une mesure d'accélération avec au moins un microsystème électromécanique de type accéléromètre, couplé au dispositif de saisie.

On peut utiliser les technologies MEMS (Microelectromechanical System, en langue anglaise), c'est-à-dire microsystème électromécanique, car elles sont largement accessibles dans le grand public. En outre, leur coût est faible. Par ailleurs, les MEMS peuvent caractériser un mouvement selon les trois axes de direction.

Plus particulièrement, les MEMS de type accéléromètre ont une taille adaptée pour un clavier d'ordinateur classique.

Selon un autre mode de mise en œuvre, la détermination de la séquence saisie comprend en outre une détermination d'une série d'au moins un identifiant de caractère saisi, la séquence de référence comporte en outre une série d'au moins un identifiant de caractère de référence, et la comparaison de séquences comprend en outre une comparaison de la série d'au moins un identifiant de caractère saisi, avec la série d'au moins un identifiant de caractère de référence.

Ainsi, on peut fournir un procédé qui utilise une authentification d'un individu par la gestuelle de l'individu et par l'utilisation d'une identification d'un mot de passe comportant une

série d'identifiants de caractères. La sécurité d'accès aux données est ainsi renforcée.

5 Selon encore un autre mode de mise en œuvre, la détermination de la séquence saisie comprend en outre une détermination d'une série d'au moins un écart temporel entre deux forces successives exercées sur le dispositif de saisie, la séquence de référence comporte en outre une série d'au moins un écart temporel de référence associé à l'utilisateur, et la comparaison de séquences comprend en outre une comparaison de la série d'au moins un écart temporel entre deux forces
10 successives exercées sur le dispositif de saisie avec la série d'au moins un écart temporel de référence.

La prise en compte d'un écart temporel, noté également « vitesse de saisie », permet de renforcer l'authentification de la gestuelle d'un individu. Ainsi on peut mesurer la force de saisie et la
15 vitesse de saisie, qui sont toutes deux des caractéristiques intrinsèques de la gestuelle d'un individu.

La détermination de la séquence de référence peut comporter une phase d'apprentissage comportant plusieurs saisies de ladite séquence de référence sur ledit dispositif de saisie et une
20 détermination desdites forces de référence à partir de ces saisies successives.

Selon encore un autre mode de mise en œuvre, la phase d'apprentissage comporte une élaboration de valeurs nominales d'une ou des forces de référence, et de valeurs de tolérance par rapport à ces
25 valeurs nominales.

Selon un autre aspect, il est proposé un système d'authentification comprenant un dispositif de saisie comportant une pluralité d'éléments de saisie configurés pour saisir respectivement des caractères en réponse à une saisie d'une séquence d'au moins un
30 caractère effectuée par un utilisateur.

Le dispositif de saisie comprend au moins un moyen de détermination, couplé à au moins un élément de saisie, pour déterminer une force exercée sur ledit au moins un élément de saisie, le système comprenant un moyen d'enregistrement pour enregistrer

une série d'au moins une force exercée sur ledit au moins un élément de saisie, une mémoire configurée pour stocker une série d'au moins une force de référence, et des moyens de comparaison configurés pour comparer la série d'au moins une force exercée avec la série d'au moins une force de référence.

Selon un mode de réalisation, le dispositif de saisie comprend plusieurs moyens de détermination, couplés respectivement à plusieurs éléments de saisie, pour déterminer une force exercée sur chaque élément de saisie, la mémoire est configurée pour stocker une série de plusieurs forces de référence et les moyens de comparaison sont configurés pour comparer la série de forces exercées avec la série de plusieurs forces de référence.

Selon un autre mode de réalisation, chaque moyen de détermination est configuré pour déterminer plusieurs forces selon plusieurs axes de direction et la mémoire est configurée pour stocker une série de plusieurs forces de référence associées à ces axes de direction.

Par exemple, les éléments de saisie sont respectivement des touches d'un clavier.

Avantageusement, au moins un moyen de détermination est un microsystème électromécanique de type accéléromètre.

Selon un mode de réalisation, le moyen d'enregistrement est en outre configuré pour enregistrer une série d'au moins un identifiant de caractère saisi, la mémoire est configurée pour stocker en outre une série d'au moins un identifiant de caractère de référence, et les moyens de comparaison sont en outre configurés pour comparer la série d'au moins un identifiant de caractère saisi avec la série d'au moins un identifiant de caractère de référence.

Selon encore un mode de réalisation, le moyen d'enregistrement est en outre configuré pour enregistrer une série d'au moins un écart temporel entre deux forces successives exercées sur les éléments de saisie, la mémoire est configurée pour stocker en outre une série d'au moins un écart temporel de référence, et les moyens de comparaison sont en outre configurés pour comparer la série d'au

moins un écart temporel enregistrée avec la série d'au moins un écart temporel de référence.

D'autres avantages et caractéristiques apparaîtront à l'examen de la description détaillée de modes de réalisation et de mise en œuvre de l'invention, nullement limitatifs, et des dessins annexés sur lesquels :

- la figure 1 illustre de façon schématique un mode de réalisation d'un système d'authentification ;
- la figure 2 illustre de façon schématique un autre mode de réalisation d'un système d'authentification ;
- et
- les figures 3a et 3b illustrent de façon schématique les principales phases d'un procédé d'authentification.

Sur la figure 1, on a représenté un système d'authentification 1 comprenant un dispositif de saisie 2 et une unité de commande électronique UCE, telle qu'un processeur et ses mémoires associées par exemple.

Le dispositif de saisie 2 peut être tout type de clavier comprenant un ensemble de touches 4. De préférence, le dispositif de saisie 2 est un clavier d'ordinateur.

Le dispositif de saisie 2 comporte une pluralité d'éléments de saisie 4. Lorsque le dispositif de saisie 2 est un clavier d'ordinateur, les éléments de saisie 4 sont les touches dudit clavier. On a représenté sur la figure 1 une vue en coupe d'une touche 4 d'un clavier d'ordinateur 2. Cette touche 4 est associée à un caractère repéré par un identifiant, par exemple {A,Z,E,R,...,N}. Cette touche 4 comprend une première zone de contact 5 sur sa face inférieure destinée à entrer en contact avec une deuxième zone de contact 6 du clavier 2. Lorsque l'utilisateur saisit un caractère à l'aide de cette touche 4, celui-ci enfonce la touche 4 et les deux zones de contact 5, 6 forment un contact électrique pour produire le caractère de la touche 4. Le signal électrique représentatif de la touche enfoncée est alors par exemple transmis au microcontrôleur du clavier 2 qui envoie l'identifiant (code

BCD, ASCII ou Unicode) de ce caractère à l'UCE, par une connexion 7. En outre, la touche 4 comporte des éléments de butée 8, 9 qui empêchent la touche 4 de sortir du clavier 2. Par ailleurs, la touche 4 est montée mobile sur des ressorts 10, 11 qui repoussent ladite touche 4 vers la partie haute 12 du clavier 2. Dans cette position, la touche 4 n'est pas enfoncée, et les éléments de butée 8, 9 sont en contact avec la partie haute 12 du clavier 2. Ainsi, lorsque l'utilisateur enfonce la touche 4, les ressorts 10 et 11 sont comprimés et les zones de contact 5 et 6 forment le contact électrique. En outre, lorsque la touche 4 est enfoncée, elle peut se déplacer, compte tenu notamment des jeux de fabrication, suivant trois axes de direction.

Par ailleurs, la touche 4 comprend un microsystème électromécanique de type accéléromètre 13, noté composant MEMS de type accéléromètre. Ce composant MEMS de type accéléromètre 13 est un composant classique accessible au public. On pourra par exemple utiliser le composant commercialisé par la société STMicroelectronics sous la référence *ST LIS3LV02TL*, qui est un capteur d'inertie MEMS de type accéléromètre permettant de détecter une accélération selon trois axes de direction, et donc une force selon les trois axes de direction.

Ce composant MEMS de type accéléromètre est couplé à l'UCE par l'intermédiaire d'une connexion 14 afin de transmettre l'information de force détectée vers l'UCE. Plusieurs, ou toutes les touches 4, peuvent être équipées d'un composant MEMS de type accéléromètre 13, en particulier les touches 4 qui seront utilisées pour saisir un mot de passe. Ce composant peut être, par exemple, collé sur la face inférieure de la touche 4 correspondante.

L'UCE, comprend un moyen d'enregistrement 20, une mémoire 21 et des moyens de comparaison 22.

Les moyens d'enregistrement 20 et de comparaison 22 peuvent être par exemple des modules logiciels au sein d'un microprocesseur de l'UCE.

Le moyen d'enregistrement 20 est couplé à la deuxième zone de contact 6 de l'élément de saisie 2 par la connexion 7. Le moyen

d'enregistrement 20 est donc configuré pour enregistrer une série d'identifiants de caractères $\{a_1, \dots, a_n\}_s$ qui a été saisie par l'utilisateur.

5 Le moyen d'enregistrement 20 est également couplé au composant MEMS de type accéléromètre 13 de la touche 4 par la connexion 14. Le moyen d'enregistrement 20 est donc configuré pour enregistrer la série de forces exercées $\{F_1, \dots, F_n\}_s$ sur les touches 4 du clavier 2 lors de la saisie de caractères. Cette série de forces exercées est associée à la série d'identifiants de caractères $\{a_1, \dots, a_n\}_s$
10 précédemment décrite.

En outre, le moyen d'enregistrement 20 est configuré pour calculer les écarts temporels Δt_i enregistrés entre deux forces successives exercées sur les touches 4 du clavier 2. On obtient ainsi une série d'écarts temporels $\{\Delta t_1, \dots, \Delta t_{n-1}\}_s$ associée à la série
15 d'identifiants de caractères $\{a_1, \dots, a_n\}_s$.

La mémoire 21 est configurée pour stocker différentes séries de référence, comme par exemple, une série d'identifiants de caractères de référence $\{a_1, \dots, a_n\}_{\text{réf}}$, une série de forces exercées de référence $\{F_1, \dots, F_n\}_{\text{réf}}$ et une série d'écarts temporels de référence $\{\Delta t_1, \dots, \Delta t_{n-1}\}_{\text{réf}}$.
20

La mémoire 21 est couplée au moyen de comparaison 22, par une transmission 24, de manière à transmettre à ce dernier les séries de référence stockées en mémoire.

25 Le moyen de comparaison 22 est également couplé au moyen d'enregistrement 20 par une connexion 25 pour recevoir les différentes séries enregistrées par ledit moyen d'enregistrement 20.

Par ailleurs, les moyens de comparaison 22 sont configurés pour comparer respectivement les séries enregistrées par le moyen d'enregistrement 20 lors de la saisie par l'utilisateur avec les séries de référence stockées dans la mémoire 21 pour authentifier ou non
30 l'utilisateur.

En effet, dans un mode de mise en œuvre très sophistiqué, l'utilisateur saisit une séquence de caractères, telle qu'un mot de passe, puis le moyen d'enregistrement 20 enregistre la série de forces

exercées $\{F_1, \dots, F_n\}_s$ sur les touches 4 utilisées lors de la saisie, et enregistre la série d'identifiants de caractères $\{a_1, \dots, a_n\}_s$ associée à la séquence saisie. En outre, le moyen d'enregistrement 20 calcule la série d'écart temporels $\{\Delta t_1, \dots, \Delta t_{n-1}\}_s$ entre deux forces successives de la série de forces exercées $\{F_1, \dots, F_n\}_s$ enregistrée. Puis, le moyen d'enregistrement 20 enregistre cette série d'écart temporels $\{\Delta t_1, \dots, \Delta t_{n-1}\}_s$ en vue de la comparer avec une série de référence. Afin d'authentifier l'individu qui a saisi la séquence de caractères, le moyen de comparaison 22 compare respectivement les séries enregistrées $\{F_1, \dots, F_n\}_s$, $\{a_1, \dots, a_n\}_s$ et $\{\Delta t_1, \dots, \Delta t_{n-1}\}_s$ avec les séries de références $\{a_1, \dots, a_n\}_{\text{réf}}$, $\{F_1, \dots, F_n\}_{\text{réf}}$ et $\{\Delta t_1, \dots, \Delta t_{n-1}\}_{\text{réf}}$ stockées dans la mémoire 21. Si les comparaisons sont correctes, l'authentification de l'individu est correcte et elle est incorrecte dans le cas contraire.

Bien entendu, l'authentification pourrait se faire uniquement à l'aide des forces mesurées, ou bien par une combinaison de ces forces avec les identifiants de caractères et/ou les vitesses de saisie.

Sur la figure 2, on a représenté un autre mode de réalisation du système d'authentification 1.

Le système d'authentification 1 comprend, un clavier d'ordinateur 2 comportant différents éléments de saisie 4 correspondant aux touches du clavier. Ce clavier 2 est également relié à un lecteur 30 de carte à microprocesseur 32 par une connexion 31. Ce lecteur 30 reçoit la carte à microprocesseur 32 qui comprend un code d'authentification, c'est-à-dire un mot de passe, crypté ou non. Par ailleurs, le clavier 2 est couplé à un ordinateur 33 via une connexion 34. En outre, l'ordinateur 33 peut également être relié à un serveur 35 via une connexion 36 qui peut être une connexion optique, électrique ou radio.

De préférence, l'UCE décrite précédemment est stockée dans l'ordinateur 33, mais d'autres configurations peuvent être envisagées.

Les séries de références peuvent être stockées dans les différents organes du système d'authentification 1. Par exemple, la

mémoire 21 peut être située dans l'ordinateur 33, dans la carte à microprocesseur 32, dans le serveur 35 ou dans le clavier 2.

En outre, le moyen de comparaison 20, qui permet de valider l'authentification de l'individu, peut également être situé dans un des organes du système d'authentification 1. Ainsi, on peut séparer l'unité
5 qui valide l'authentification des moyens qui stockent les séries de référence.

Sur les figures 3a et 3b, on a représenté les principales étapes du procédé d'authentification.

10 Ce procédé comprend une étape S1 de saisie d'une séquence de caractères, telle qu'un mot de passe, par l'utilisateur.

Lors de cette étape S1 de saisie, on effectue une étape S11 de détermination d'une série de forces exercées sur le dispositif de saisie $\{F1, \dots, Fn\}_s$.

15 Cette étape S1 de saisie comprend ici en outre une détermination S12 d'une série d'identifiants de caractères saisis $\{a1, \dots, an\}_s$.

Cette étape S1 de saisie peut également comprendre une détermination S13 d'une série d'écarts temporels entre deux forces
20 successives exercées $\{\Delta t_1, \dots, \Delta t_{n-1}\}_s$.

Le procédé d'authentification de l'utilisateur comprend également une étape S2 dans laquelle on détermine des séries de référence en vue de comparer les séries déterminées lors de la saisie de la séquence de caractères avec des références.

25 La détermination d'une séquence de référence S2 comprend une détermination S21 d'une série de forces de référence $\{F1, \dots, Fn\}_{\text{réf}}$, et également dans cet exemple une détermination S22 d'une série d'identifiants de caractères de référence $\{a1, \dots, an\}_{\text{réf}}$ et une détermination S23 d'une série d'écarts temporels de référence $\{\Delta t_1, \dots,$
30 $\Delta t_{n-1}\}_{\text{réf}}$.

La détermination S22 de la série d'identifiants de caractères de référence $\{a1, \dots, an\}_{\text{réf}}$ comprend un stockage en mémoire de ladite série, c'est-à-dire un enregistrement d'un mot de passe.

Pour déterminer la série de forces de référence, le procédé d'authentification peut comprendre une phase d'apprentissage S4 comportant une première étape S41 où l'utilisateur effectue plusieurs saisies d'une même séquence de caractères, et une deuxième étape S42 où l'on élabore des valeurs nominales des forces exercées et des valeurs de tolérance.

La phase d'apprentissage S4 peut être effectuée préalablement à toute saisie « opérationnelle » par l'utilisateur, ou bien au cours par exemple d'au moins les premières saisies « opérationnelles » par l'utilisateur.

L'élaboration S42 des valeurs nominales des forces exercées et des valeurs de tolérance peut être effectuée à partir d'un test statistique. Ce test statistique permet d'établir un profil de forces associé à l'utilisateur. Un exemple de test possible est notamment décrit. Selon cet exemple de test, on peut considérer, par exemple, un mot de passe de dix caractères $\{a_1, \dots, a_{10}\}_s$. L'utilisateur saisit ces dix caractères et pour chaque événement, c'est-à-dire pour chaque touche du clavier enfoncée, on mesure la valeur d'une force exercée $F_{i,k}$, où i est un index représentant la touche enfoncée par l'utilisateur, et k un index représentant la saisie effectuée. Ainsi, lors d'une première saisie, on obtient la série de forces $\{F_{1,1} ; \dots F_{10,1}\}_s$, lors de la deuxième saisie on obtient la deuxième série de forces $\{F_{1,2} ; \dots F_{10,2}\}_s$, lors de la k -ième saisie on obtient la k -ième série de forces $\{F_{1,k} ; \dots F_{10,k}\}_s$.

On peut ensuite combiner ces valeurs de forces en faisant la moyenne arithmétique pour obtenir des valeurs de référence $\{F_1, \dots F_{10}\}_{\text{réf}}$. En outre, on calcule l'écart type D_i des valeurs des forces $F_{i,k}$ obtenues pour obtenir les valeurs nominales $\{F_1 \pm D_1, \dots F_{10} \pm D_{10}\}_{\text{réf}}$. Cette série de valeurs nominales $\{F_1 \pm D_1, \dots F_{10} \pm D_{10}\}_{\text{réf}}$ est ensuite enregistrée comme une série de forces de référence $\{F_1, \dots, F_{10}\}_{\text{réf}}$, avec $F_1 = F_1 \pm D_1, \dots, F_{10} = F_{10} \pm D_{10}$.

On peut en outre utiliser une tolérance V que l'on peut fixer, par exemple à 5%, pour caractériser les saisies de l'utilisateur. On

détermine alors une série de forces de référence correspondant à la série d'intervalles suivante $\{F1 \pm (D1 + V), \dots, F10 \pm (D10 + V)\}$ réf.

On peut appliquer un test statistique identique pour déterminer la série d'écarts temporels de référence
 5 $\{\Delta t_1 \pm (D1 + Vt), \dots, \Delta t_9 \pm (D9 + Vt)\}$ réf, où la tolérance Vt peut être égale à la tolérance V utilisée pour la série de référence précédente.

Comme indiqué ci avant, dans un premier mode de mise en œuvre, les séries de référence peuvent être stockées en mémoire préalablement à la saisie de la séquence de caractères (saisie
 10 « opérationnelle »). Puis on effectue, à l'étape S3, une comparaison des séries saisies avec les séries de référence pour authentifier l'utilisateur.

Dans un autre mode de mise en œuvre, on stocke en mémoire la série d'identifiant de caractères de référence $\{a_1, \dots, a_n\}$ réf et on
 15 détermine les séries de forces de référence $\{F1, \dots, F_n\}$ réf, et d'écarts temporels de référence $\{\Delta t_1, \dots, \Delta t_{n-1}\}$ réf au cours de, ou de toutes, les saisies « opérationnelles » effectuées par l'utilisateur. Ainsi, on peut préciser les valeurs nominales de ces deux séries de référence tout au long de l'utilisation du clavier par l'individu de manière à renforcer
 20 l'authentification.

La comparaison de séquences S3 comporte dans cet exemple trois étapes de comparaison S31 à S33. La première étape de comparaison S31 permet de comparer la série de forces exercées sur le dispositif de saisie $\{F1, \dots, F_n\}_s$, avec la série de forces de référence
 25 $\{F1, \dots, F_n\}$ réf. Si la comparaison est correcte, on effectue alors la deuxième étape de comparaison S32 et sinon, on effectue une étape d'erreur S35, où l'on déclare l'authentification comme incorrecte.

On entend par identification correcte, le fait que la force exercée F_i lors de la saisie est comprise dans l'intervalle déterminé à partir du test statistique. Autrement dit, on compare les forces exercées mesurées $\{F1, \dots, F_n\}_s$ avec les forces de référence
 30 $\{F1 \pm (D1 + V), \dots, F_n \pm (D_n + V)\}$ réf.

Si les valeurs des forces exercées F_i appartiennent à l'intervalle $[F_i - (D_i + V), F_i + (D_i + V)]$, alors on estime que la comparaison est correcte.

5 Dans la deuxième étape de comparaison S32, on compare la série des identifiants de caractères saisis $\{a_1, \dots, a_n\}_s$ avec la série d'identifiants de caractères de référence $\{a_1, \dots, a_n\}_{\text{réf}}$. Lors de cette étape S32, si la série d'identifiants de caractères saisis est identique à la série d'identifiants de caractères de référence, on effectue la troisième étape de comparaison S33 et l'on effectue l'étape d'erreur S35 sinon. Cette étape permet de renforcer l'authentification.

10 Lors de la troisième étape de comparaison S33, on compare la série d'écarts temporels saisis $\{\Delta t_1, \dots, \Delta t_{n-1}\}_s$ avec la série d'écarts temporels de référence $\{\Delta t_1, \dots, \Delta t_{n-1}\}_{\text{réf}}$. Si la comparaison est correcte, on effectue une étape de validité S34 dans laquelle on déclare l'authentification correcte et l'on effectue l'étape d'erreur S35 sinon.

Bien entendu, l'ordre des deuxième S32 et troisième S33 étapes peut être inversé.

REVENDICATIONS

1. Procédé d'authentification comprenant une détermination (S1) d'une séquence d'au moins un caractère saisie par un utilisateur sur un dispositif de saisie de caractères, une détermination (S2) d'une
5 séquence d'au moins un caractère de référence et une comparaison (S3) de la séquence saisie avec la séquence de référence, caractérisé en ce que la détermination (S1) de la séquence saisie comporte une détermination (S11) d'une série d'au moins une force exercée sur le dispositif de saisie lors de la saisie de la séquence, la détermination
10 (S2) de la séquence de référence comporte une détermination (S21) d'une série d'au moins une force de référence associée à l'utilisateur, et ladite comparaison de séquences (S3) comporte une comparaison (S31) de la série d'au moins une force exercée sur le dispositif de saisie avec la série d'au moins une force de référence.
- 15 2. Procédé selon la revendication 1, dans lequel la détermination (S1) de la séquence saisie comprend une détermination (S11) d'une série de plusieurs forces exercées successivement sur le dispositif de saisie, la détermination (S2) de la séquence de référence comporte la détermination (S21) d'une succession de plusieurs forces
20 de référence associée à l'utilisateur et ladite comparaison de séquences (S3) comporte une comparaison (S31) de ladite série de forces exercées sur le dispositif de saisie avec ladite succession de forces de référence.
- 25 3. Procédé selon la revendication 2, dans lequel la détermination (S1) de la séquence saisie comprend la détermination (S11) d'une série de plusieurs forces exercées sur le dispositif de saisie selon plusieurs axes de direction, et la séquence de référence comporte une série de plusieurs forces de référence associées à ces axes de direction.
- 30 4. Procédé selon l'une des revendications précédentes, dans lequel la détermination (S11) de la ou les forces exercées sur le dispositif de saisie, ainsi que la ou les forces de référence, comportent

au moins une mesure d'accélération avec au moins un microsystème électromécanique de type accéléromètre couplé au dispositif de saisie.

5 5. Procédé selon l'une des revendications précédentes, dans lequel la détermination (S1) de la séquence saisie comprend en outre
10 une détermination (S12) d'une série d'au moins un identifiant de caractère saisi, la séquence de référence comporte en outre une série d'au moins un identifiant de caractère de référence, et la comparaison de séquences (S3) comprend en outre une comparaison (S32) de la
15 série d'au moins un identifiant de caractère saisi avec la série d'au moins un identifiant de caractère de référence.

 6. Procédé selon l'une des revendications précédentes, dans lequel la détermination (S1) de la séquence saisie comprend en outre
une détermination (S13) d'une série d'au moins un écart temporel
15 entre deux forces successives exercées sur le dispositif de saisie, la séquence de référence comporte en outre une série d'au moins un écart temporel de référence associée à l'utilisateur, et la comparaison de séquences (S3) comprend en outre une comparaison (S33) de la série
d'au moins un écart temporel entre deux forces successives exercées
20 sur le dispositif de saisie avec la série d'au moins un écart temporel de référence.

 7. Procédé selon l'une des revendications précédentes, dans lequel la détermination (S2) de la séquence de référence comporte une
phase d'apprentissage (S4) comportant plusieurs saisies (S41) de ladite
séquence de référence sur ledit dispositif de saisie et une
25 détermination (S21) desdites forces de référence à partir de ces saisies successives.

 8. Procédé selon la revendication 7, dans lequel la phase
d'apprentissage (S4) comporte une élaboration (S42) de valeurs
nominales d'une ou des forces de référence, et de valeurs de tolérance
30 par rapport à ces valeurs nominales.

 9. Système d'authentification comprenant un dispositif de
saisie (2) comportant une pluralité d'éléments de saisie (4) configurés
pour saisir respectivement des caractères en réponse à une saisie d'une
séquence d'au moins un caractère effectuée par un utilisateur,

caractérisé en ce que le dispositif de saisie (2) comprend au moins un moyen de détermination (13), couplé à au moins un élément de saisie (4), pour déterminer une force exercée sur ledit au moins un élément de saisie (4), le système comprenant un moyen d'enregistrement (20)
5 pour enregistrer une série d'au moins une force exercée sur ledit au moins un élément de saisie (4), une mémoire (21) configurée pour stocker une série d'au moins une force de référence, et des moyens de comparaison (22) configurés pour comparer la série d'au moins une force exercée avec la série d'au moins une force de référence.

10 10. Système selon la revendication 9, dans lequel le dispositif de saisie (2) comprend plusieurs moyens de détermination (13), couplés respectivement à plusieurs éléments de saisie (4), pour déterminer une force exercée sur chaque élément de saisie (4), la mémoire (21) est en outre configurée pour stocker une série de
15 plusieurs forces de référence et les moyens de comparaison (22) sont configurés pour comparer la série de forces exercées avec la série de plusieurs forces de référence.

11. Système selon la revendication 10, dans lequel chaque moyen de détermination (13) est configuré pour déterminer plusieurs
20 forces selon plusieurs axes de direction et la mémoire (21) est configurée pour stocker une série de plusieurs forces de référence associées à ces axes de direction.

12. Système selon l'une des revendications 9 à 11, dans lequel les éléments de saisie (4) sont respectivement des touches d'un clavier
25 (2).

13. Système selon l'une des revendications 9 à 12, dans lequel au moins un moyen de détermination (13) est un microsystème électromécanique de type accéléromètre.

14. Système selon l'une des revendications 9 à 13, dans lequel
30 le moyen d'enregistrement (20) est en outre configuré pour enregistrer une série d'au moins un identifiant de caractère saisi, la mémoire (22) est configurée pour stocker en outre une série d'au moins un identifiant de caractère de référence, et les moyens de comparaison (22) sont en outre configurés pour comparer la série d'au moins un

identifiant de caractère saisi avec la série d'au moins un identifiant de caractère de référence.

- 5 15. Système selon l'une des revendications 9 à 14, dans lequel le moyen d'enregistrement (20) est en outre configuré pour enregistrer une série d'au moins un écart temporel entre deux forces successives exercées sur les éléments de saisie, la mémoire (21) est configurée pour stocker en outre une série d'au moins un écart temporel de référence, et les moyens de comparaison (22) sont en outre configurés pour comparer la série d'au moins un écart temporel enregistrée avec
10 la série d'au moins un écart temporel de référence.

1/3
FIG.1

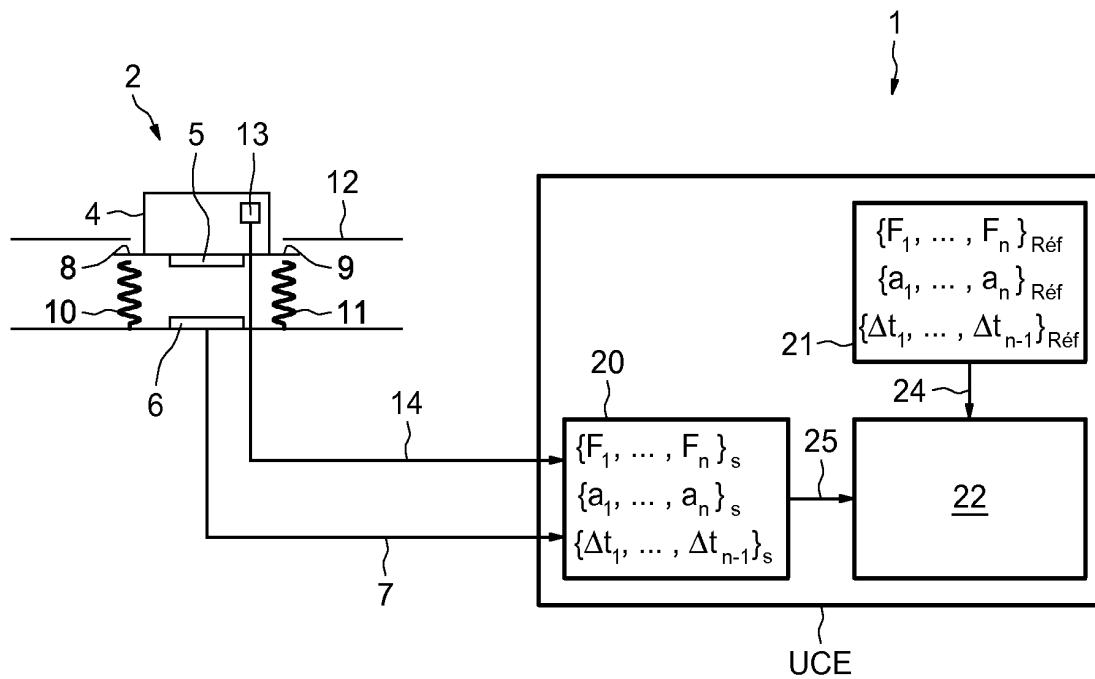
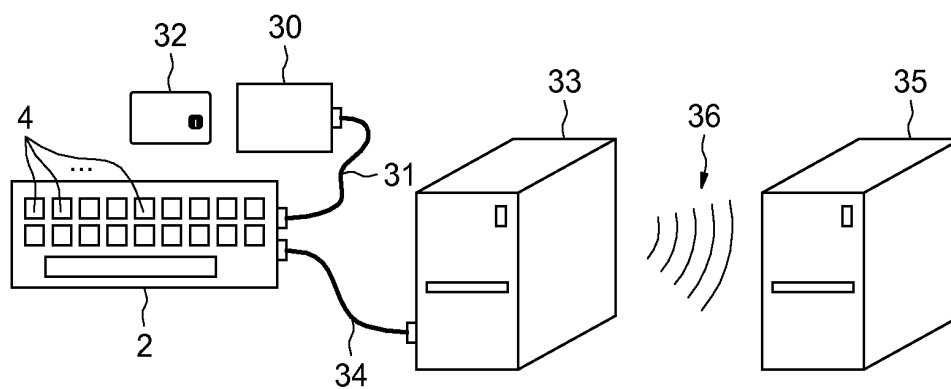
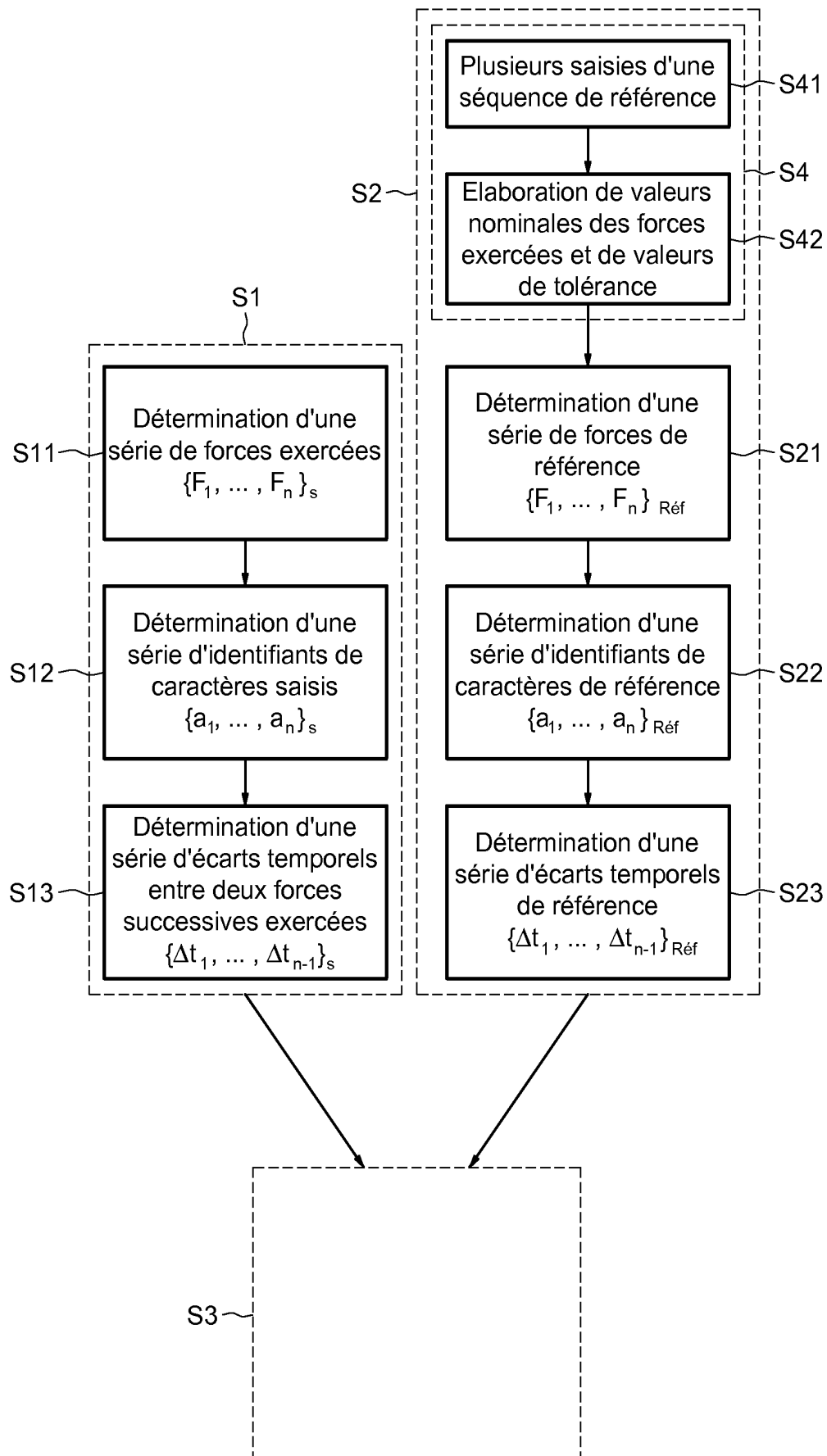
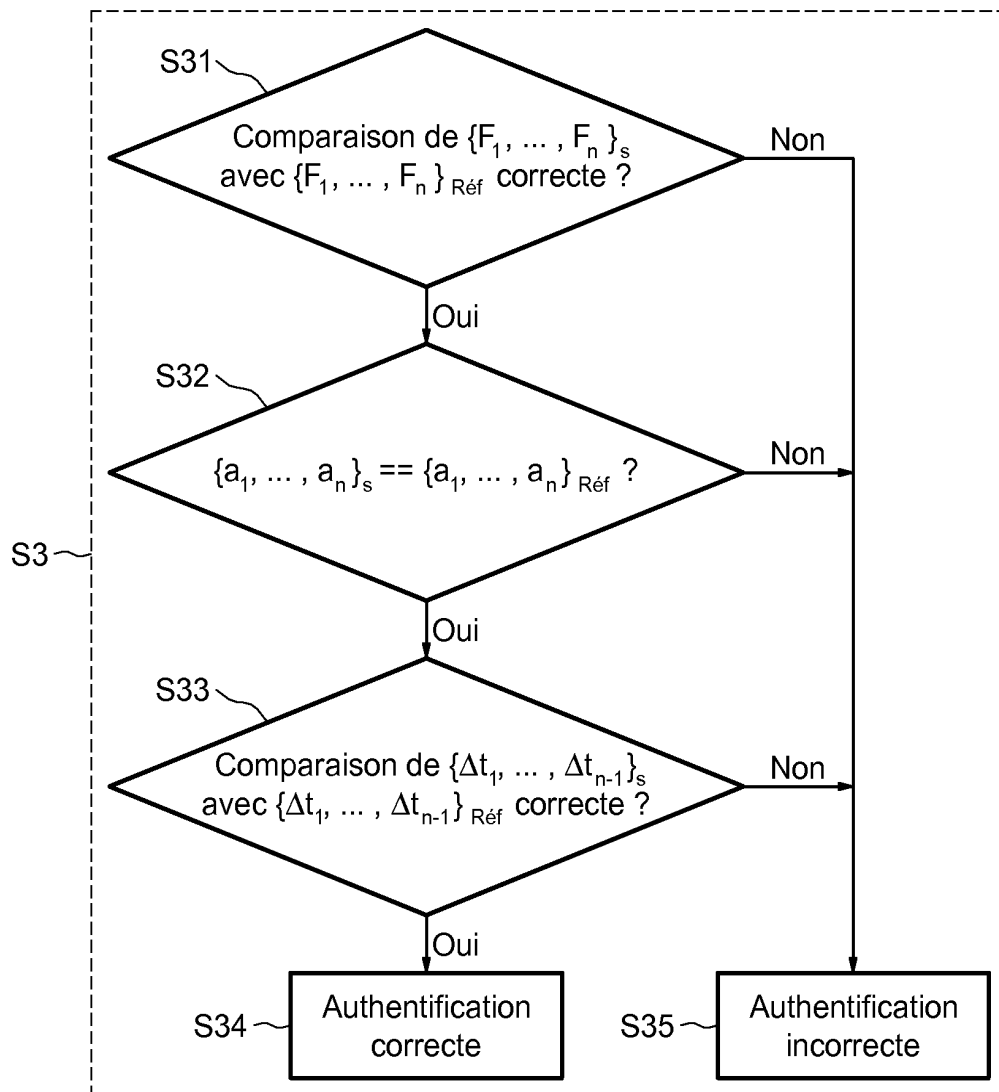


FIG.2



2/3
FIG.3a

3/3
FIG.3b





RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement
national

FA 739935
FR 1053059

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	US 5 995 026 A (SELLERS CHARLES A [US]) 30 novembre 1999 (1999-11-30) * colonne 1, ligne 55 - colonne 3, ligne 17 * * colonne 8, ligne 12 - colonne 9, ligne 5 *	1-15	G06K9/00 G01L1/00
X	EP 1 469 372 A2 (AT & T CORP [US]) 20 octobre 2004 (2004-10-20) * colonne 6 * * colonne 8 - colonne 21 *	1-15	
A	WO 03/032551 A1 (LITRONIC INC [US]) 17 avril 2003 (2003-04-17) * page 3, ligne 16 - page 5, ligne 33 *	1-15	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			G06F
Date d'achèvement de la recherche		Examineur	
9 décembre 2010		Pinto, Raúl	
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			

**ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE
RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1053059 FA 739935**

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 **09-12-2010**

Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 5995026	A	30-11-1999	AUCUN	
EP 1469372	A2	20-10-2004	CA 2464449 A1	16-10-2004
WO 03032551	A1	17-04-2003	US 2003070100 A1	10-04-2003