(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 987 152**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **12 51593**

(51) Int Cl[8] : ***G 06 K 19/07*** *(2013.01), G 06 Q 20/00*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 22.02.12.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 23.08.13 Bulletin 13/34.

(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) :** *OBERTHUR TECHNOLOGIES Société anonyme* — FR.

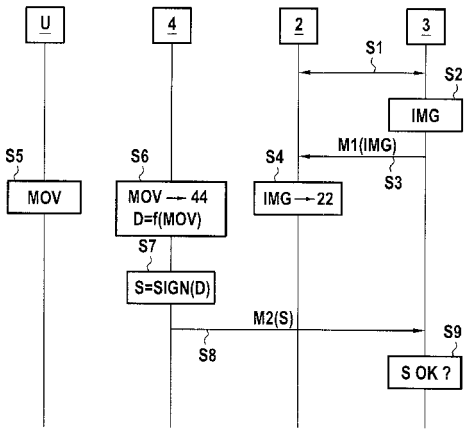
(72) **Inventeur(s) :** DABOSVILLE GUILLAUME, DOTTAX EMMANUELLE, SIERRA YANNICK, DOS SANTOS ELDER, CONDEMINE OLIVIER et LAAZIMANI OMAR.

(73) **Titulaire(s) :** OBERTHUR TECHNOLOGIES Société anonyme.

(74) **Mandataire(s) :** CABINET BEAU DE LOMENIE Société civile.

(54) PROCEDE ET DISPOSITIF DE SECURITE POUR EFFECTUER UNE TRANSACTION.

(57) Procédé pour déterminer la présence d'un être humain, comprenant :
- la mesure (S6) d'un mouvement (MOV) d'un premier dispositif (4) par un capteur (44) dudit premier dispositif (4) ;
- la détermination de la présence d'un être humain sur la base du mouvement (MOV) mesuré.



FR 2 987 152 - A1

Domaine de l'invention

L'invention se rapporte au domaine des transactions impliquant une communication entre le terminal d'un utilisateur et un serveur.

Contexte de l'invention

Lorsqu'une transaction se fait entre le terminal d'un utilisateur et un serveur, il est généralement souhaitable que le serveur authentifie l'utilisateur. Les techniques habituelles pour authentifier un utilisateur sont l'utilisation d'un identifiant et d'un mot de passe, d'une signature cryptographique calculée par un élément de sécurité comme une carte de module d'identité d'abonné (SIM pour "Subscriber Identity Module"), etc.

De plus, en considérant la possibilité qu'un programme informatique malveillant habituellement connu comme un logiciel malveillant peut s'exécuter sur le terminal d'utilisateur, il est aussi souhaitable que le serveur vérifie que la transaction se fait sur ordre de l'utilisateur.

Une technique habituelle pour vérifier qu'une transaction se fait sur ordre d'un utilisateur (d'un être humain) consiste en un test de défi/réponse connu sous le nom de CAPTCHA (pour "Completely Automated Public Turing test to tell Computers and Humans Apart"). Typiquement, le serveur envoie au terminal une image qui comprend des caractères alphanumériques qui sont difficiles à reconnaître pour un programme de reconnaissance optique des caractères (OCR pour "Optical Character Recognition"), mais visibles pour un être humain. Le terminal affiche l'image et l'utilisateur entre les caractères alphanumériques. Le serveur vérifie que les caractères entrés correspondent à l'image.

Cependant, une attaque est toujours possible et en vérité, certains logiciels de reconnaissance de caractères ont été développés pour reconnaître l'information dans une image de CAPTCHA.

Donc, il est souhaitable d'améliorer les techniques pour vérifier qu'une transaction se fait sur ordre d'un utilisateur.

Résumé et objectif de l'invention

Pour déterminer la présence d'un être humain, l'invention propose un procédé comprenant :

- la mesure d'un mouvement d'un premier dispositif par un capteur dudit premier dispositif ;
- la détermination de la présence d'un être humain sur la base du mouvement mesuré.

Dans un mode de réalisation, le procédé comprend la sortie d'un stimuli sur une interface d'utilisateur, le stimuli comprenant des instructions pour effectuer un mouvement prédéterminé,

dans lequel la détermination de la présence d'un être humain sur la base du mouvement mesuré comprend la détermination de la présence d'un être humain sur la base du mouvement mesuré et du mouvement prédéterminé.

Le procédé peut comprendre :

- la transmission du stimuli d'un serveur à ladite interface d'utilisateur ;
- la détermination, par ledit premier dispositif, d'une signature sur la base du mouvement mesuré ;
- la transmission de ladite signature du premier dispositif au serveur.

Le procédé peut comprendre :

- la transmission de premières données d'un serveur audit premier dispositif ;
- la détermination, par ledit premier dispositif, dudit stimuli sur la base desdites premières données ;
- la détermination, par ledit premier dispositif, de ce que le mouvement mesuré et le mouvement prédéterminé concordent ou non ;

- si le mouvement mesuré et le mouvement prédéterminé concordent, la détermination, par ledit premier dispositif, d'une signature sur la base des premières données ;
- la transmission de ladite signature du premier dispositif au serveur.

Lesdites premières données peuvent comprendre un montant d'une transaction de paiement.

Ledit premier dispositif peut être un élément de sécurité.

La sortie du stimuli sur l'interface d'utilisateur peut comprendre la sortie du stimuli sur l'interface d'utilisateur d'un second dispositif différent dudit premier dispositif.

Dans un mode de réalisation, le procédé comprend :
- la détermination de données de transaction sur la base du mouvement mesuré ;
- la détermination, par ledit premier dispositif, d'une signature sur la base desdites données de transaction ;
- la transmission de ladite signature du premier dispositif à un serveur.

Lesdites données de transaction peuvent comprendre un montant d'une transaction de paiement.

Dans un mode de réalisation, le premier dispositif est constitué pour autoriser l'exécution d'une fonction protégée par authentification à la réception de données d'identification ou d'authentification entrées par un utilisateur, le procédé comprenant la détermination desdites données d'identification ou d'authentification sur la base du mouvement mesuré.

Le premier dispositif peut avoir un premier état dans lequel il accepte les données d'identification ou d'authentification entrées sur une interface d'utilisateur d'un second dispositif et un second état dans lequel il n'accepte pas les données d'identification ou d'authentification entrées sur ladite interface d'utilisateur, le procédé comprenant une étape de commutation dudit premier état audit second état en réponse à la

détection de ce que le second dispositif effectue une transaction prédéterminée.

Pour déterminer la présence d'un être humain, l'invention propose aussi un système comprenant :

- un premier dispositif comprenant un capteur apte à mesurer un mouvement dudit premier dispositif ;
-des moyens aptes à déterminer la présence d'un être humain sur la base du mouvement mesuré.

Le système peut comprendre un second dispositif ayant une interface d'utilisateur apte à sortir un stimuli, le stimuli comprenant des instructions pour effectuer un mouvement prédéterminé, dans lequel les moyens aptes à déterminer la présence d'un être humain sont constitués pour déterminer la présence d'un être humain sur la base du mouvement mesuré et du mouvement prédéterminé.

Le premier dispositif peut être un élément de sécurité inséré dans ledit second dispositif.

Brève description des dessins

Ces objectifs et particularités, ainsi que d'autres, de la présente invention deviendront clairs à partir de la description suivante des modes préférés de réalisation donnée en se référant aux dessins annexés, dans lesquels :

- la figure 1 montre un système selon un mode de réalisation de l'invention ;
- la figure 2 est un diagramme d'enchaînement d'une transaction dans le système de la figure 1, selon un premier mode de réalisation de l'invention ;
- la figure 3 est un diagramme d'enchaînement d'une transaction dans le système de la figure 1, selon un deuxième mode de réalisation de l'invention ;

- la figure 4 est un diagramme d'enchaînement d'une transaction dans le système de la figure 1, selon un troisième mode de réalisation de l'invention ;
- la figure 5 est un diagramme d'enchaînement d'une transaction dans le système de la figure 1, selon un quatrième mode de réalisation de l'invention ;
- la figure 6 est un diagramme d'enchaînement d'une transaction dans le système de la figure 1, selon un cinquième mode de réalisation de l'invention ;
- la figure 7 est un diagramme d'enchaînement d'une transaction dans le système de la figure 1, selon un sixième mode de réalisation de l'invention ;
- la figure 8 illustre un procédé pour entrer un numéro personnel d'identification (PIN pour "Personal Identification Number") dans le système de la figure 1.

Description détaillée de modes préférés de réalisation

La figure 1 montre un système 1 qui comprend un terminal 2, un serveur 3, et un élément de sécurité 4. Dans un exemple de mode de réalisation, le terminal 2 est le téléphone mobile d'un utilisateur (un être humain), le serveur 3 est un terminal de paiement de point de vente et l'élément 2 de sécurité est une carte intelligente insérée dans le terminal, par exemple une carte SIM. Cependant, l'invention n'est pas limitée à ce mode de réalisation. Par exemple, le terminal 2 peut être un ordinateur personnel, un dispositif électronique portatif, etc.. Le serveur 3 peut être un guichet automatique (ATM pour "Automated Teller Machine") ou un serveur du Web. L'élément de sécurité 4 peut être une clé USB connectée au terminal 2 ou un dispositif distinct qui communique avec le terminal 2 par une connexion sans fil ou filaire. Également, le terminal 2 et le serveur 3 peuvent être le même dispositif.

Le terminal 2 présente l'architecture générale d'un ordinateur. Il comprend une interface d'utilisateur 21 qui inclut par exemple un écran 22 et un clavier 23 ou un écran tactile, un processeur 24, une mémoire non volatile 25, une mémoire volatile 26, une interface de communication 27 et une interface de communication 28. Le processeur 24 permet, en utilisant la mémoire volatile 26, l'exécution de programmes informatiques mémorisés dans la mémoire non volatile 25. Le fonctionnement du terminal 2 décrit ci-après correspond à l'exécution de tels programmes informatiques.

L'interface de communication 27 permet la communication entre le terminal 2 et le serveur 3 par l'intermédiaire d'une liaison L1. Par exemple, l'interface de communication 27 est une interface de communication par radio à courte portée, par exemple une interface de communication en champ proche (NFC pour "Near Field Communication") qui inclut un frontal de NFC et une antenne de NFC. Dans d'autres modes de réalisation, l'interface de communication 27 est configurée pour communication avec le serveur 3 par l'intermédiaire d'un réseau filaire ou sans fil, par exemple par l'Internet et/ou par un réseau de téléphonie mobile.

L'interface de communication 28 permet la communication entre le terminal 2 et l'élément de sécurité 4 par l'intermédiaire d'une liaison L2. Dans l'exemple d'une carte intelligente insérée dans le terminal 3, la liaison L2 est par exemple une liaison normalisée ISO 7816.

L'élément de sécurité 4 présente l'architecture générale d'un ordinateur. Il comprend un processeur 41, une mémoire non volatile 42, une mémoire volatile 43, un capteur 44 et une interface de communication 45. Le processeur 41 permet, en utilisant la mémoire volatile 43, l'exécution de programmes informatiques mémorisés dans la mémoire non volatile 42. Le fonctionnement de l'élément de sécurité 4

décrit ci-après correspond à l'exécution de tels programmes informatiques. L'interface de communication 45 permet la communication entre le terminal 2 et l'élément de sécurité 4 par l'intermédiaire de la liaison L2. La mémoire non volatile 42 mémorise un code PIN et une clé de cryptographie K de l'utilisateur. Le capteur 44 est par exemple un microcapteur électromécanique (MEMS pour "Micro ElectroMechanical Sensor"), un accéléromètre, une boussole, etc., constitué pour mesurer un mouvement, une orientation ou une position de l'élément de sécurité 2.

Les liaisons L1 et L2 permettent la communication entre l'élément de sécurité 4 et le serveur 2 par l'intermédiaire d'une liaison L3, qui est basée par exemple sur des protocoles monofilaires (SWP pour "Single Wire Protocol") et qui autorise la communication entre un frontal de NFC l'élément de sécurité 4.

Le serveur 3 présente l'architecture générale d'un ordinateur. Il comprend un processeur 31, une mémoire non volatile 32, une mémoire volatile 33 et une interface de communication 34. Le processeur 31 permet, en utilisant la mémoire volatile 33, l'exécution de programmes informatiques mémorisés dans la mémoire non volatile 32. Le fonctionnement du serveur 3 décrit ci-après correspond à l'exécution de tels programmes informatiques. L'interface de communication 34 permet la communication entre le terminal 2 et le serveur 3 par l'intermédiaire de la liaison L1.

Dans le système de la figure 1, l'élément de sécurité 4 est considéré comme un environnement plus sûr que le terminal 2. En réalité, l'installation de nouvelles applications par chargement de programmes informatiques dans la mémoire non volatile 25 du terminal 2 est une tâche usuelle qui peut se faire par l'utilisateur du terminal 2. L'installation d'une nouvelle application dans le terminal 2 peut entraîner, à l'insu de l'utilisateur, l'installation d'un logiciel malveillant. Donc, un logiciel

malveillant peut s'exécuter sur le terminal 2. Au contraire, le chargement d'un programme informatique dans la mémoire non volatile 42 de l'élément de sécurité 4 peut se faire seulement après authentification par une entité autorisée, par exemple le fabricant ou l'émetteur de l'élément de sécurité ou une tierce partie de confiance. En d'autres termes, l'élément de sécurité 4 comprend des moyens pour autoriser le chargement d'un programme informatique dans sa mémoire non volatile 42 seulement après authentification par une entité autorisée. Donc, normalement il n'y a pas de logiciel malveillant s'exécutant sur l'élément de sécurité 4.

La figure 2 est un diagramme d'enchaînement d'une transaction dans le système 1 de la figure 1, selon un premier mode de réalisation de l'invention.

Initialement, l'utilisateur U lance une transaction avec le serveur 3 (étape S1). Ceci peut impliquer une communication bidirectionnelle entre le terminal 2 et le serveur 3. Dans un autre mode de réalisation, l'utilisateur U utilise un autre dispositif que le terminal 2 pour communication avec le serveur 3, et spécifie la façon dont le serveur 3 peut contacter le terminal 2. Par exemple, l'utilisateur U utilise un ordinateur personnel pour lancer la transaction avec un serveur du Web, et spécifie son numéro de téléphone.

Ensuite, lorsque la transaction doit être validée en confirmant qu'elle est effectuée sur ordre de l'utilisateur U, le serveur 3 détermine une image IMG (étape S2) et envoie au terminal 2 un message M1 contenant l'image IMG (étape S3). L'image IMG contient des instructions pour que l'utilisateur effectue un mouvement spécifique MOV. On va décrire ci-après un exemple de relation entre les instructions contenues dans l'image IMG et le mouvement MOV.

En réponse à la réception du message M1, le terminal 2 affiche l'image IMG sur l'écran 22 (étape S4). Ensuite, l'utilisateur U effectue le mouvement MOV ordonné par l'image IMG (étape S5) tandis que le capteur 44 mesure le mouvement MOV et que l'élément de sécurité 4 détermine des données D sur la base du mouvement MOV mesuré (étape S6).

Ensuite, l'élément de sécurité 2 détermine une signature S en signant les données D (S=SIGN(D)) à l'aide de la clé de cryptographie K (étape S7) et envoie au serveur 3 un message M2 contenant la signature S (étape S8). Dans une variante, le message M2 est d'abord envoyé de l'élément de sécurité 2 à un dispositif de sécurité (non représenté) et ensuite du dispositif de sécurité au serveur 3 ceci s'applique aussi aux modes de réalisation décrits ci-après.

Finalement, le serveur 3 vérifie si la signature S correspond à l'image IMG de l'étape S2 (étape S9). Par exemple, le serveur 3 vérifie si la signature S est une signature par l'utilisateur U des données D' correspondant aux instructions de l'image IMG. Ici, les données D' représentent les données qui doivent être déterminées à l'étape S6 si l'utilisateur U effectue le mouvement correct. La transaction est validée (S OK) seulement si la signature S correspond à l'image IMG de l'étape S2.

Le procédé de la figure 2 permet de vérifier que la transaction est effectuée sur ordre de l'utilisateur U. En réalité, un logiciel malveillant qui s'exécuterait sur le terminal 2 aurait accès à l'image IMG, mais pas au mouvement MOV qui est mesuré sur l'élément de sécurité 4 ni à la clé de cryptographie K qui est mémorisée sur l'élément de sécurité 2. Ainsi, le logiciel malveillant serait incapable d'engendrer une signature S correspondant à l'image IMG à l'insu de l'utilisateur U.

La figure 3 est un diagramme d'enchaînement d'une transaction dans le système 1 de la figure 1, selon un deuxième mode de réalisation de l'invention.

Initialement, l'utilisateur U lance une transaction avec le serveur 3 (étape S11). Comme à la figure 2, ceci peut impliquer une communication bidirectionnelle entre le terminal 2 et le serveur 3, ou bien l'utilisateur U peut utiliser un autre dispositif que le terminal 2 pour communication avec le serveur 3, et spécifier la façon dont le serveur 3 peut contacter le terminal 2.

Ensuite, lorsque la transaction a besoin d'être validée en confirmant qu'elle est effectuée sur ordre de l'utilisateur U, le serveur 3 détermine un défi CHAL (étape S12) et envoie à l'élément de sécurité 4 un message M3 contenant le défi CHAL (étape S13). Le défi CHAL est, par exemple, un nombre déterminé d'une manière pseudo-aléatoire et/ou sur la base de données de transaction.

En réponse à la réception du message M3, l'élément de sécurité 4 détermine une image IMG (étape S14) sur la base du défi CHAL. Comme à la figure 2, l'image IMG contient des instructions pour que l'utilisateur effectue un mouvement MOV spécifique. Ensuite, l'élément de sécurité 4 envoie au terminal 2 un message M4 contenant l'image IMG (étape S15).

En réponse à la réception du message M4, le terminal 2 affiche l'image IMG sur l'écran 22 (étape S16). Puis, l'utilisateur U effectue le mouvement MOV ordonné par l'image IMG (étape S17) tandis que le capteur 44 mesure le mouvement MOV et que l'élément de sécurité 4 détermine des données D sur la base du mouvement MOV mesuré (étape S18).

L'élément de sécurité 4 détermine si les données D correspondent au mouvement MOV ordonné par l'image IMG (étape S19). Par exemple, l'élément de sécurité 4 compare les données D avec les données D'

représentant les données qui doivent être déterminées à l'étape S18 si l'utilisateur U effectue le mouvement correct.

S'il est déterminé à l'étape S19 que les données D correspondent au mouvement MOV ordonné par l'image IMG, l'élément de sécurité 4 détermine une signature S en signant le défi CHAL à l'aide de la clé de cryptographie K (étape S20) et envoie au serveur 3 un message M5 contenant la signature S (étape S21).

Finalement, le serveur 3 vérifie si la signature S correspond au défi CHAL de l'étape S12 (étape S22). La transaction est validée seulement si la signature S correspond au défi CHAL de l'étape S12.

Le procédé de la figure 3 permet de vérifier que la transaction est effectuée sur ordre de l'utilisateur U. En réalité, un logiciel malveillant qui s'exécuterait sur le terminal 2 aurait accès à l'image IMG, mais pas au mouvement MOV qui est mesuré sur l'élément de sécurité 4 ni à la clé de cryptographie K qui est mémorisée sur l'élément de sécurité 2, ni au défi CHAL qui n'est pas transmis au terminal 2. Ainsi, le logiciel malveillant serait incapable d'engendrer une signature S correspondant au défi CHAL à l'insu de l'utilisateur U.

Dans une variante du procédé de la figure 3, à l'étape S17, l'utilisateur U effectue un mouvement MOV1 qui correspond à l'image IMG, et un mouvement MOV2 qui correspond à son PIN. On va décrire ci-après une technique pour effectuer un mouvement qui correspond à un PIN. À l'étape S18, on mesure les deux mouvements MOV1 et MOV2, on détermine les données D sur la base de MOV1 et d'un PIN entré, à noter que le PIN' est déterminé sur la base de MOV2. Ensuite, les données D et le PIN' sont vérifiés à l'étape S19.

La figure 4 est un diagramme d'enchaînement d'une transaction dans le système 1 de la figure 1, selon un troisième mode de réalisation de l'invention.

Initialement, l'utilisateur U lance une transaction avec le serveur 3 (étape S31). Dans cet exemple, la transaction est une transaction de paiement d'un montant A déterminé par le serveur 3 (étape 32) et implique une communication bidirectionnelle entre le terminal 2 et le serveur 3.

Ensuite, lorsque la transaction a besoin d'être validée en confirmant qu'elle est effectuée sur ordre de l'utilisateur U, le serveur 3 envoie à l'élément de sécurité 4 un message M6 contenant le montant A (étape S33).

En réponse à la réception du message M6, l'élément de sécurité 4 détermine une image IMG (étape S34) sur la base du montant A. L'image IMG contient des instructions pour que l'utilisateur effectue un mouvement MOV spécifique et le montant A. Ensuite, l'élément de sécurité 4 envoie au terminal 2 un message M7 contenant l'image IMG (étape S35).

En réponse à la réception du message M7, le terminal 2 affiche l'image IMG sur l'écran 22 (étape S36). Ensuite, si l'utilisateur U accepte le montant A affiché dans l'image IMG, il effectue le mouvement MOV ordonné par l'image IMG (étape S37) tandis que le capteur 44 mesure le mouvement MOV et que l'élément de sécurité 4 détermine des données D sur la base du mouvement MOV mesuré (étape S38).

Ensuite, l'élément de sécurité 2 détermine si les données D correspondent au mouvement MOV ordonné par l'image IMG (étape S39).

S'il est déterminé à l'étape S39 que les données D correspondent au mouvement MOV ordonné par l'image IMG, l'élément de sécurité 4 détermine une signature S en signant le montant A à l'aide de la clé de cryptographie K (étape S40) et envoie au serveur 3 un message M41 contenant la signature S (étape S41).

Ici, le message M6 qui inclut le montant A et le message M8 qui inclut la signature du montant A peuvent être des messages conformes aux normes de paiement, par exemple aux normes Europay MasterCard & Visa (EMV).

Finalement, le serveur 3 vérifie si la signature S correspond au montant A de l'étape S32 (étape S42). La transaction est validée seulement si la signature S correspond au montant A de l'étape S32.

Le procédé de la figure 4 permet de vérifier que la transaction est effectuée sur ordre de l'utilisateur U et que l'utilisateur accepte le montant A. En réalité, un logiciel malveillant qui s'exécuterait sur le terminal 2 aurait accès à l'image IMG, mais pas au mouvement MOV qui est mesuré sur l'élément de sécurité 4 ni à la clé de cryptographie K qui est mémorisée sur l'élément de sécurité 2. Ainsi, le logiciel malveillant serait incapable d'engendrer une signature S correspondant au montant A à l'insu de l'utilisateur U. De plus, au cas où le logiciel malveillant essaierait de modifier le montant indiqué dans l'image affichée, ceci modifierait aussi, par effet indirect, l'instruction associée au mouvement à effectuer. Le mouvement effectué par l'utilisateur U ne serait pas reconnu par l'élément de sécurité 4 à l'étape S39 et par conséquent l'élément de sécurité 4 ne déterminerait pas la signature S.

La figure 5 est un diagramme d'enchaînement d'une transaction dans le système 1 de la figure 1, selon un quatrième mode de réalisation de l'invention.

Initialement, l'utilisateur U lance une transaction avec le serveur 3 (étape S51). Dans cet exemple, la transaction est une transaction de paiement d'un montant A déterminé par le serveur 3 (étape 52) et implique une communication bidirectionnelle entre le terminal 2 et le serveur 3.

Ensuite, lorsque la transaction a besoin d'être validée en confirmant qu'elle est effectuée sur ordre de l'utilisateur U, le serveur 2 envoie à l'élément de sécurité 4 un message M9 contenant le montant A (étape S53). De plus, le terminal 2 invite l'utilisateur à entrer le montant A' accepté pour la transaction (étape S54).

Donc, en réponse à l'étape S54, l'utilisateur U effectue un mouvement MOV représentatif du montant A'. Par exemple, l'utilisateur U utilise le terminal 2 qui inclut l'élément de sécurité 4 comme un stylo pour écrire le montant A'. Dans une variante, le montant A' est entré d'une manière similaire à l'entrée d'un PIN décrite ci-après. Dans le même temps, le capteur 44 de l'élément de sécurité 4 mesure le mouvement MOV et l'élément de sécurité 4 détermine un montant A' à partir du mouvement MOV mesuré par le capteur 44 (étape S56). Ensuite, l'élément de sécurité 4 compare le montant A' avec le montant A du message M9 (étape S57).

Si A' = A, l'élément de sécurité 4 détermine une signature S en signant le montant A à l'aide de la clé de cryptographie K (étape S58) et envoie au serveur 3 un message M10 contenant la signature S (étape S59).

Ici, le message M9 qui inclut le montant A et le message M10 qui inclut la signature du montant A peuvent être des messages conformes aux normes de paiement, par exemple aux normes EMV.

Finalement, le serveur 3 vérifie si la signature S correspond au montant A de l'étape S52 (étape S60). La transaction est validée seulement si la signature S correspond au montant A de l'étape S52.

Le procédé de la figure 5 permet de vérifier que la transaction est effectuée sur ordre de l'utilisateur U et que l'utilisateur accepte le montant A. En réalité, un logiciel malveillant qui s'exécuterait sur le terminal 2 n'aurait pas accès au mouvement MOV ni au montant A ni à la clé de

cryptographie K. Ainsi, le logiciel malveillant serait incapable d'engendrer une signature S correspondant au montant A à l'insu de l'utilisateur U.

La figure 6 est un diagramme d'enchaînement d'une transaction dans le système 1 de la figure 1, selon un cinquième mode de réalisation de l'invention.

Initialement, l'utilisateur U lance une transaction avec le serveur 3 (étape S71). Dans cet exemple, la transaction est une transaction de paiement d'un montant A.

Ensuite, le terminal 2 invite l'utilisateur à entrer le montant A accepté pour la transaction (étape S72).

Donc, en réponse à l'étape S72, l'utilisateur U effectue un mouvement MOV représentatif du montant A (étape S73). Dans le même temps, le capteur 44 de l'élément de sécurité 4 mesure le mouvement MOV et l'élément de sécurité 4 détermine un montant A à partir du mouvement MOV mesuré par le capteur 44 (étape S74). Ensuite, l'élément de sécurité 4 détermine une signature S en signant le montant A à l'aide de la clé de cryptographie K (étape S75) et envoie au serveur 3 un message M11 contenant la signature S et le montant A (étape S76).

Finalement, le serveur 3 vérifie si la signature S correspond au montant A du message M11 (étape S77). La transaction est validée seulement si la signature S correspond au montant A du message M11.

Le procédé de la figure 6 permet de vérifier que la transaction est effectuée sur ordre de l'utilisateur U et que l'utilisateur accepte le montant A. En réalité, un logiciel malveillant qui s'exécuterait sur le terminal 2 n'aurait pas accès au mouvement MOV ni au montant A ni à la clé de cryptographie K. Ainsi, le logiciel malveillant serait incapable d'engendrer une signature S correspondant au montant A à l'insu de l'utilisateur U.

La figure 7 est un diagramme d'enchaînement d'une transaction dans le système 1 de la figure 1, selon un sixième mode de réalisation de l'invention.

Dans ce mode de réalisation, l'élément de sécurité 4 commande l'exécution de fonctions protégées par authentification. L'élément de sécurité 4 est constitué pour comparer des données d'identification ou d'authentification entrées par un utilisateur avec des données d'identification ou d'authentification qui y sont mémorisées, et autorise l'exécution d'une fonction protégée seulement si les données entrées et mémorisées concordent. Dans cet exemple, les données d'identification ou d'authentification comprennent un PIN. De plus, un premier type de fonction protégée peut être autorisé en entrant le PIN sur l'interface d'utilisateur 21 du terminal 2, tandis qu'un second type de fonction protégée peut être autorisé seulement en entrant le PIN comme décrit ci-après. Dans cet exemple, une fonction protégée du premier type comprend l'authentification auprès d'un réseau de téléphonie mobile, et une fonction protégée du second type comprend la validation d'une transaction, par exemple une transaction de paiement.

Initialement, l'élément de sécurité 4 est dans un état ST1 où il accepte un PIN entré par l'utilisateur U sur l'interface d'utilisateur 21. Par exemple, lorsque le terminal 2 est mis en marche, l'élément de sécurité 4 entre dans l'état ST1 (étape S90). Ensuite, l'utilisateur U entre son PIN sur le clavier 23 (étapes S91 et S92) et le PIN est transmis à l'élément de sécurité 4 (étape S93), par exemple dans une instruction ADPU de la norme ISO 7816. Si le PIN transmis concorde avec le PIN mémorisé dans la mémoire non volatile 42, l'élément de sécurité 4 autorise l'authentification auprès du réseau de téléphonie mobile (étape S94). En d'autres termes, l'authentification auprès du réseau de téléphonie mobile est une fonction protégée du premier type mentionné ci-dessus.

Plus tard, l'utilisateur U lance une transaction avec le serveur 3 (étape S95). Ceci peut impliquer une communication bidirectionnelle entre le terminal 2 et le serveur 3.

À l'étape S96, l'élément de sécurité 4 détecte le lancement de la transaction et passe dans un état S2 où il n'accepte pas un PIN entré sur l'interface d'utilisateur 21.

Ensuite, le serveur 3 envoie à l'élément de sécurité 4 un message M12, contenant des données T associées à la transaction (étape S97). Par exemple, d'une manière similaire au message M6 de la figure 4, les données T contiennent un montant A.

L'élément de sécurité 4 est constitué pour approuver la transaction en signant les données T seulement si l'utilisateur U entre son PIN. Cependant, à l'état ST2, l'utilisateur ne peut pas transmettre son PIN à l'élément de sécurité 4 en l'entrant sur l'interface d'utilisateur 21. En d'autres termes, l'approbation de la transaction est une fonction protégée du second type mentionné ci-dessus.

Donc, à l'étape S98, l'utilisateur U effectue un mouvement MOV correspondant à son PIN. Le mouvement MOV est mesuré par le capteur 44 et l'élément de sécurité 4 détermine un PIN entré, désigné par PIN', sur la base du mouvement MOV mesuré (étape S99). Ensuite, l'élément de sécurité 4 détermine si le PIN' et le PIN mémorisé dans la mémoire non volatile 42 concordent (étape S100).

Dans le cas où les PIN concordent, l'élément de sécurité 4 détermine une signature S en signant les données T à l'aide de la clé de cryptographie K (étape S101) et envoie au serveur 4 un message M13 contenant la signature S (étape S102).

Ici, le message M12 qui inclut les données T et le message M13 qui inclut la signature des données T peuvent être des messages conformes aux normes de paiement, par exemple aux normes EMV.

Finalement, le serveur 3 vérifie si la signature S correspond aux données T du message M12 (étape S103). La transaction est validée seulement si la signature S correspond aux données T du message M12.

Le procédé de la figure 7 permet de vérifier que la transaction est effectuée sur ordre de l'utilisateur U et que l'utilisateur accepte les données T. En réalité, un logiciel malveillant qui s'exécuterait sur le terminal 2 n'aurait pas accès aux données T, au mouvement MOV ni à la clé de cryptographie K. Ainsi, le logiciel malveillant serait incapable d'engendrer une signature S correspondant aux données T. De plus, au cas où le logiciel malveillant essaierait d'envoyer un PIN à partir du terminal 2 à l'élément de sécurité 4, ce PIN ne serait pas accepté par l'élément de sécurité 4 parce qu'il serait entré dans l'état ST2 à la détection du début de la transaction. Ainsi, même si un logiciel malveillant intercepte le PIN de l'utilisateur (par exemple à l'étape S92), la transaction ne peut pas être validée par le logiciel malveillant à l'insu de l'utilisateur. En d'autres termes, une fonction protégée du second type est plus sûre.

La figure 8 représente un exemple de la façon dont un utilisateur peut effectuer un mouvement MOV correspondant à des instructions affichées dans une image IMG (par exemple aux étapes S5, S17, S37) à un montant A ou A' (par exemple aux étapes S55, S73) ou à son PIN (par exemple à l'étape S37 de la variante mentionnée ci-dessus ou à l'étape S98) et de la façon dont l'élément de sécurité 4 peut déterminer des données D, un montant A ou A' ou un PIN' (par exemple aux étapes S6, S18, S38, S56, S74, S99) sur la base du mouvement mesuré.

Dans cet exemple, le capteur 44 est une boussole capable de mesurer l'orientation de l'élément de sécurité 4 et par conséquent du terminal 2. L'élément de sécurité 4 transmet périodiquement au terminal 2 l'orientation mesurée par le capteur 44.

Le terminal 2 affiche une image sur l'écran 22 comprenant un cadran 210 et une flèche 211. Le cadran 210 comprend des caractères alphanumériques, dans cet exemple les chiffres 0 à 9. La flèche 211 est affichée à une position fixe tandis que le terminal 2 commande l'affichage du cadran en se basant sur l'orientation mesurée par le capteur 44. Ainsi, comme le montre la figure 8, lorsque l'utilisateur effectue un mouvement qui change l'orientation du terminal 2, le chiffre du cadran 210 indiqué par la flèche 211 change.

Lorsque l'utilisateur fait tourner le terminal 2 de façon que la flèche 211 indique un chiffre spécifique du cadran 210 et arrête dans cette position, l'élément de sécurité 4 considère que ce chiffre spécifique a été entré. En répétant ceci, l'utilisateur peut effectuer un mouvement MOV comprenant une pluralité de rotations et d'arrêts et qui correspond, pour l'élément de sécurité 4, à une suite de chiffres. Cette suite de chiffres représente des données déterminées sur la base du mouvement MOV, au sens de la présente invention.

Dans l'exemple de la figure 8, le cadran de 210 est une image prédéterminée où les chiffres 0 à 9 sont affichés dans l'ordre. Cependant, le cadran 210 pourrait être une image déterminée par l'élément de sécurité 4 où des caractères alphanumériques seraient affichés dans un ordre aléatoire. Dans ce cas, il n'est pas possible pour un logiciel malveillant s'exécutant sur le terminal de déterminer les données D, les montants A/A' ou le PIN' à partir de l'orientation transmise par l'élément de sécurité 4 afin de commander l'affichage du cadran.

Dans certains des modes de réalisation ci-dessus, une image comprend de l'information pour ordonner à l'utilisateur d'effectuer un mouvement spécifique et elle est affichée par le terminal. Dans une variante, l'information pour ordonner à l'utilisateur d'effectuer le

mouvement est comprise dans un autre type de stimuli, par exemple un son ou une vibration, qui est sorti par le terminal.

REVENDICATIONS

1. Système (1) apte à déterminer la présence d'un être humain, comprenant :

- un premier dispositif (4) comprenant un capteur (44) apte à mesurer (S6, S18, S38, S56, S74, S99) un mouvement (MOV) dudit premier dispositif (4) ;
- des moyens aptes à déterminer la présence d'un être humain sur la base du mouvement (MOV) mesuré.

2. Système selon la revendication 1, comprenant un second dispositif (2) ayant une interface d'utilisateur (21) apte à sortir un stimuli, le stimuli comprenant des instructions pour effectuer un mouvement prédéterminé, dans lequel les moyens aptes à déterminer la présence d'un être humain sont constitués pour déterminer la présence d'un être humain sur la base du mouvement mesuré et du mouvement prédéterminé.

3. Système selon la revendication 2, comprenant un serveur (3) comprenant des moyens aptes à transmettre (S3) le stimuli du serveur (3) à ladite interface d'utilisateur (21), dans lequel le premier dispositif (4) comprend :

- des moyens aptes à déterminer (S7) une signature (S) sur la base du mouvement mesuré ;
- des moyens aptes à transmettre (S8) ladite signature (S) du premier dispositif (4) à un dispositif de sécurité ou au serveur (3).

4. Système selon la revendication 2, comprenant un serveur (3) comprenant des moyens aptes à transmettre (S13, S33) des premières données (CHAL, A) du serveur (3) audit premier dispositif (4), dans lequel le premier dispositif (4) comprend :

- des moyens aptes à déterminer (S14, S34) ledit stimuli (IMG) sur la base desdites premières données (CHAL, A) ;

- des moyens aptes à déterminer (S19, S39) si le mouvement mesuré et le mouvement prédéterminé concordent ;
- des moyens aptes à déterminer (S20, S40), si le mouvement mesuré et le mouvement prédéterminé concordent, une signature (S) sur la base des premières données (CHAL, A) ;
- des moyens aptes à transmettre (S21, S41) ladite signature (S) du premier dispositif (4) à un dispositif de sécurité ou au serveur (3).

5. Système selon la revendication 4, dans lequel lesdites premières données comprennent un montant (A) d'une transaction de paiement.

6. Système selon l'une des revendications 2 à 5, dans lequel ledit premier dispositif (4) est un élément de sécurité.

7. Système selon la revendication 6, dans lequel le second dispositif (2) est différent dudit premier dispositif (4).

8. Système selon la revendication 1, comprenant des moyens aptes à déterminer (S56, S74) des données de transaction (A, A') sur la base du mouvement mesuré, dans lequel le premier dispositif (4) comprend :
- des moyens aptes à déterminer (S58, S75) une signature (S) sur la base desdites données de transaction (A, A') ;
- des moyens aptes à transmettre (S59, S76) ladite signature (S) du premier dispositif (4) à un dispositif de sécurité ou à un serveur (3).

9. Système selon la revendication 6, dans lequel lesdites données de transaction comprennent un montant (A) d'une transaction de paiement.

10. Système selon l'une des revendications 8 à 9, dans lequel, ledit premier dispositif (4) est un élément de sécurité.

11. Système selon la revendication 1, dans lequel le premier dispositif (4) est constitué pour autoriser l'exécution d'une fonction

protégée par authentification à la réception de données d'identification ou d'authentification entrées par un utilisateur, le système comprenant des moyens aptes à déterminer (S99) lesdites données d'identification ou d'authentification sur la base du mouvement mesuré.

12. Système selon la revendication 11, dans lequel le premier dispositif (4) a un premier état (ST1) dans lequel il accepte les données d'identification ou d'authentification entrées sur une interface d'utilisateur (21) d'un second dispositif (2) et un second état (ST2) dans lequel il n'accepte pas les données d'identification ou d'authentification entrées sur ladite interface d'utilisateur (21), le système comprenant des moyens de commutation dudit premier état (ST1) audit second état (ST2) en réponse à la détection (S96) de ce que le second dispositif (2) effectue une transaction prédéterminée.

13. Système selon la revendication 12, dans lequel ledit premier dispositif (4) est un élément de sécurité.

14. Procédé pour déterminer la présence d'un être humain, comprenant :

- la mesure (S6, S18, S38, S56, S74, S99) d'un mouvement (MOV) d'un premier dispositif (4) par un capteur (44) dudit premier dispositif (4) ;
- la détermination de la présence d'un être humain sur la base du mouvement (MOV) mesuré.

15. Procédé selon la revendication 14, comprenant :

- la sortie (S4, S16, S36) d'un stimuli (IMG) sur une interface d'utilisateur (21), le stimuli comprenant des instructions pour effectuer un mouvement prédéterminé,

dans lequel la détermination de la présence d'un être humain sur la base du mouvement mesuré comprend la détermination de la présence d'un être humain sur la base du mouvement mesuré et du mouvement prédéterminé.

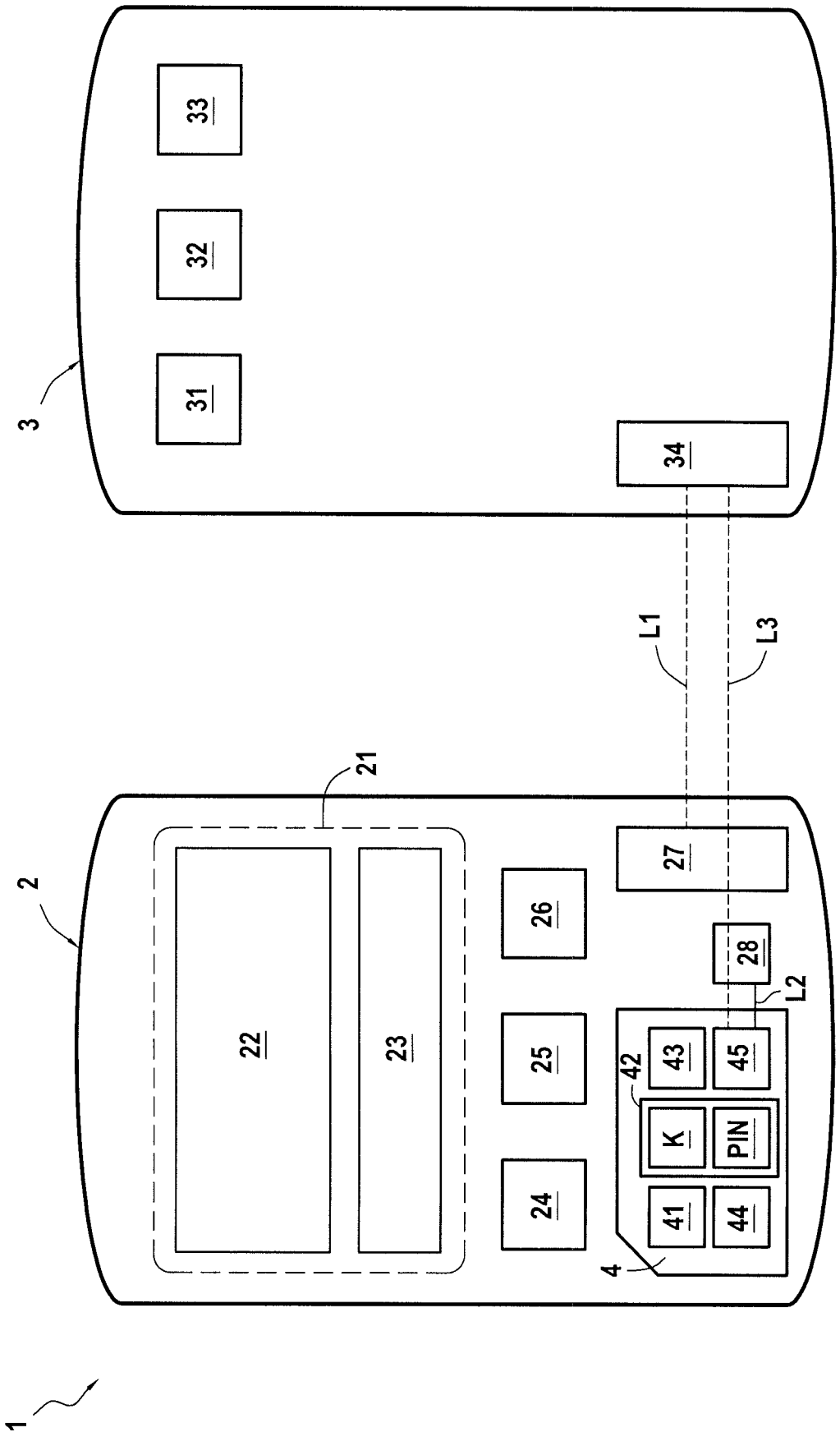


FIG.1

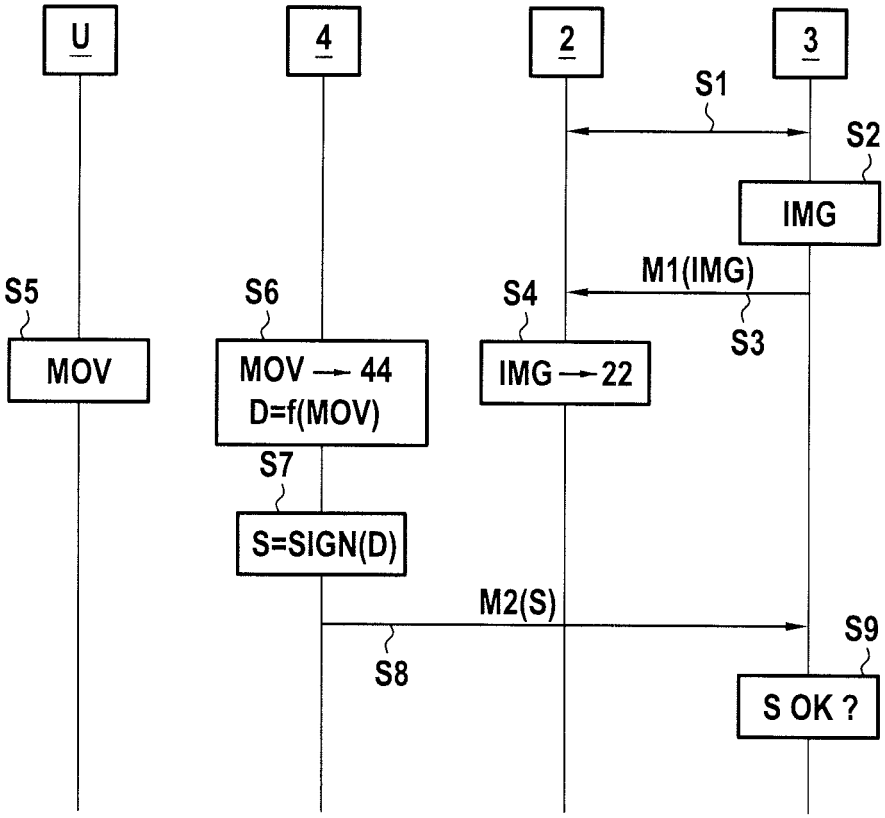

U
4
2
3
S1
S2
IMG
M1(IMG)
S3
S5
S6
S4
MOV
MOV → 44
D=f(MOV)
IMG → 22
S7
S=SIGN(D)
M2(S)
S8
S9
S OK ?

FIG.2

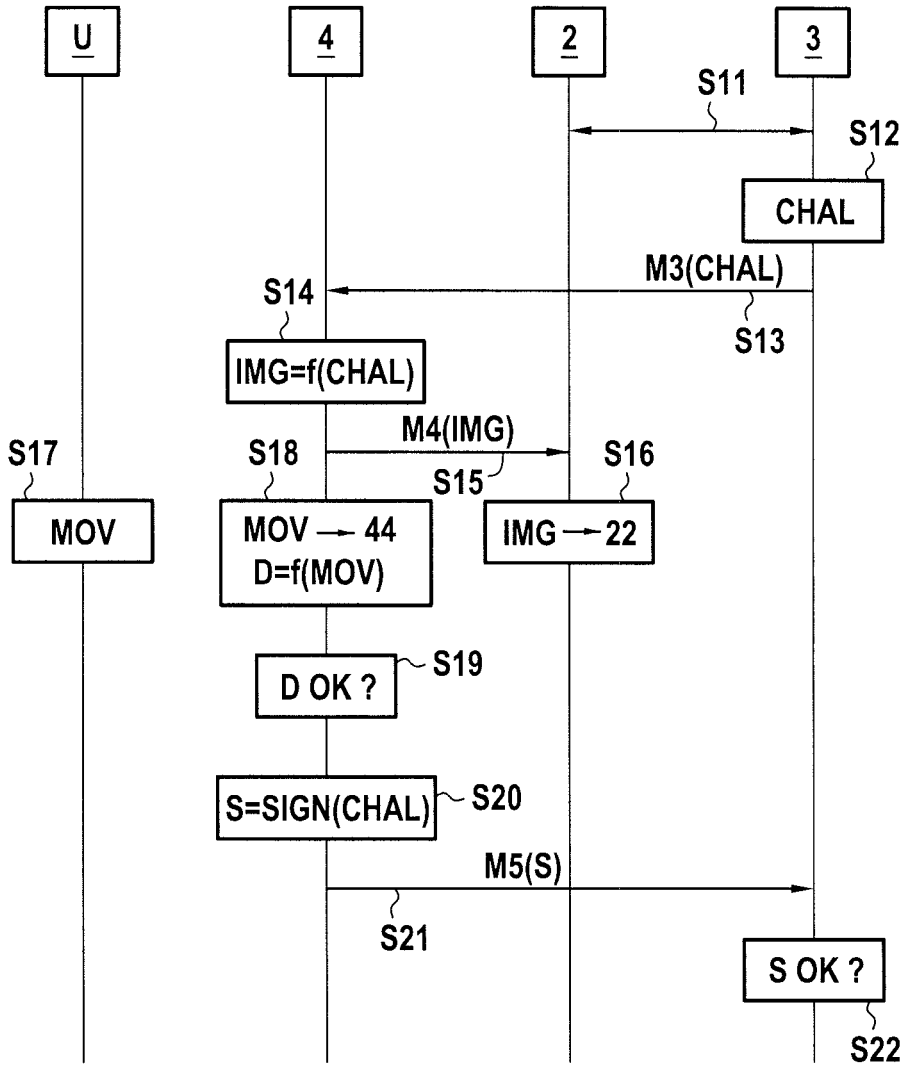

U
4
2
3
S11
S12
CHAL
M3(CHAL)
S14
S13
IMG=f(CHAL)
M4(IMG)
S17
S18
S15
S16
MOV
MOV → 44
D=f(MOV)
IMG → 22
D OK ?
S19
S=SIGN(CHAL)
S20
M5(S)
S21
S OK ?
S22

FIG.3

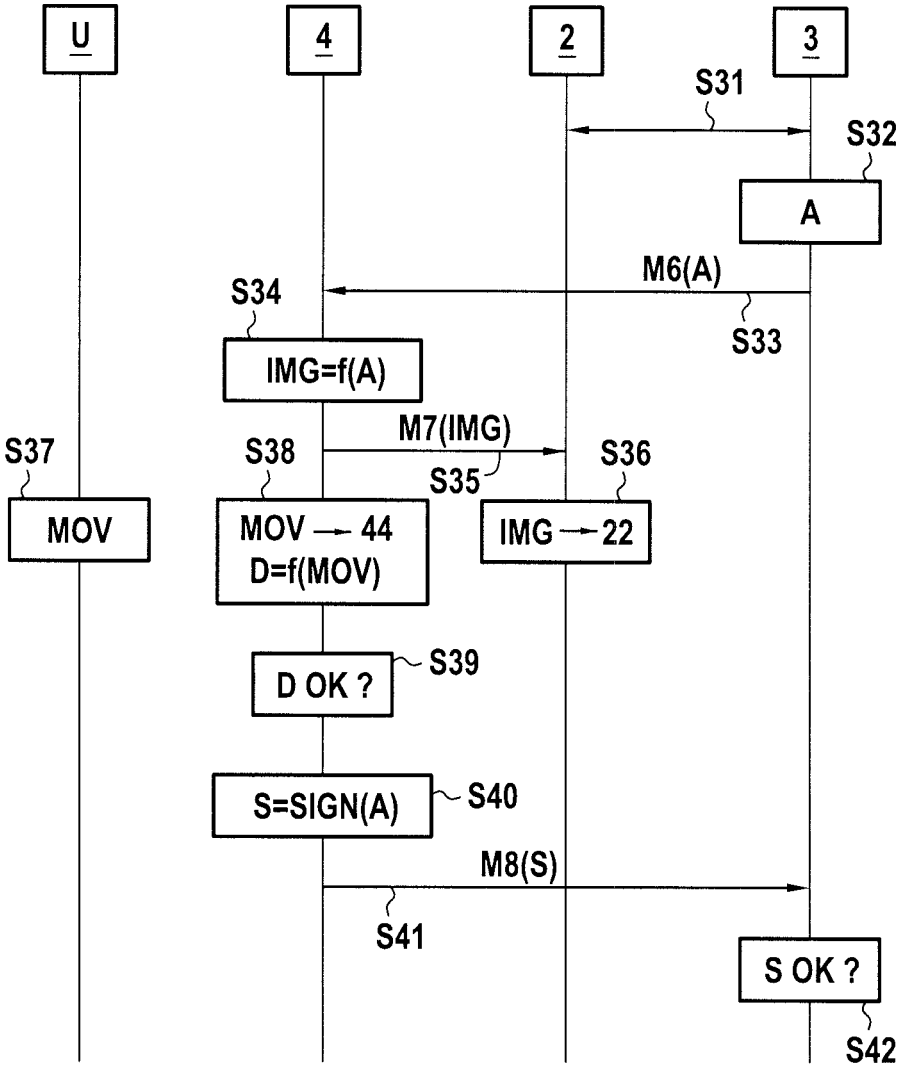

U
4
2
3
S31
S32
A
M6(A)
S34
S33
IMG=f(A)
M7(IMG)
S37
S38
S35
S36
MOV
MOV → 44
D=f(MOV)
IMG → 22
D OK ?
S39
S=SIGN(A)
S40
M8(S)
S41
S OK ?
S42

FIG.4

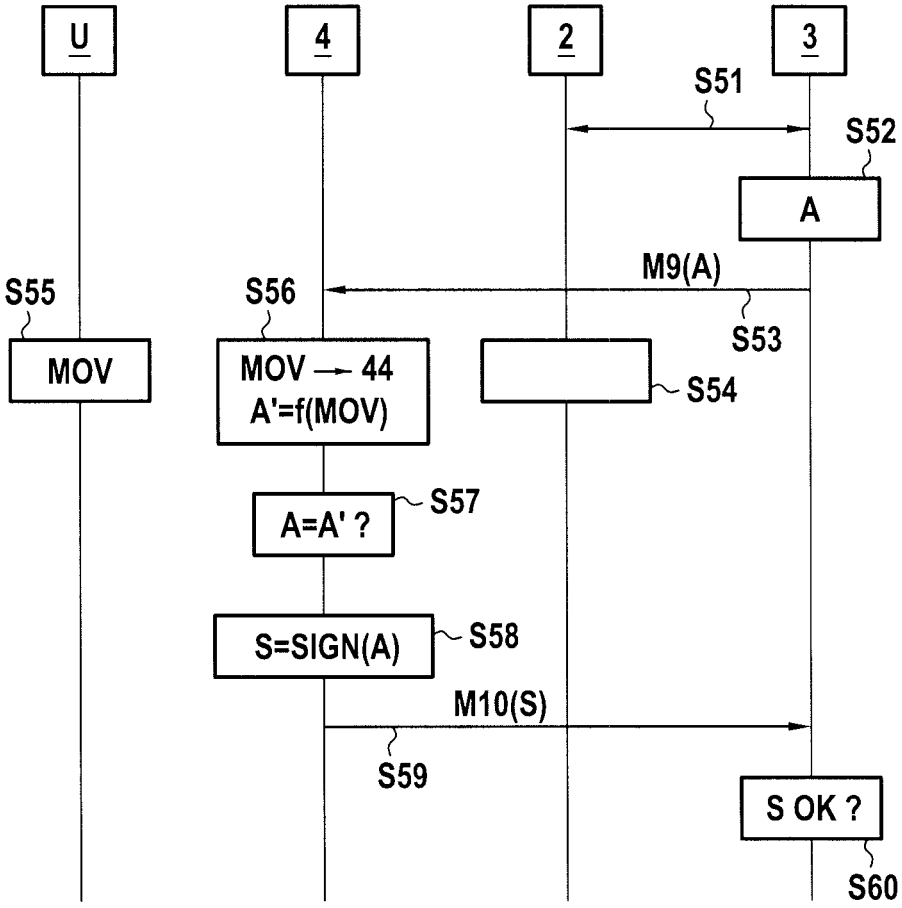

U
4
2
3
S51
S52
A
M9(A)
S55
S56
S53
MOV
MOV → 44
A'=f(MOV)
S54
A=A' ?
S57
S=SIGN(A)
S58
M10(S)
S59
S OK ?
S60

FIG.5

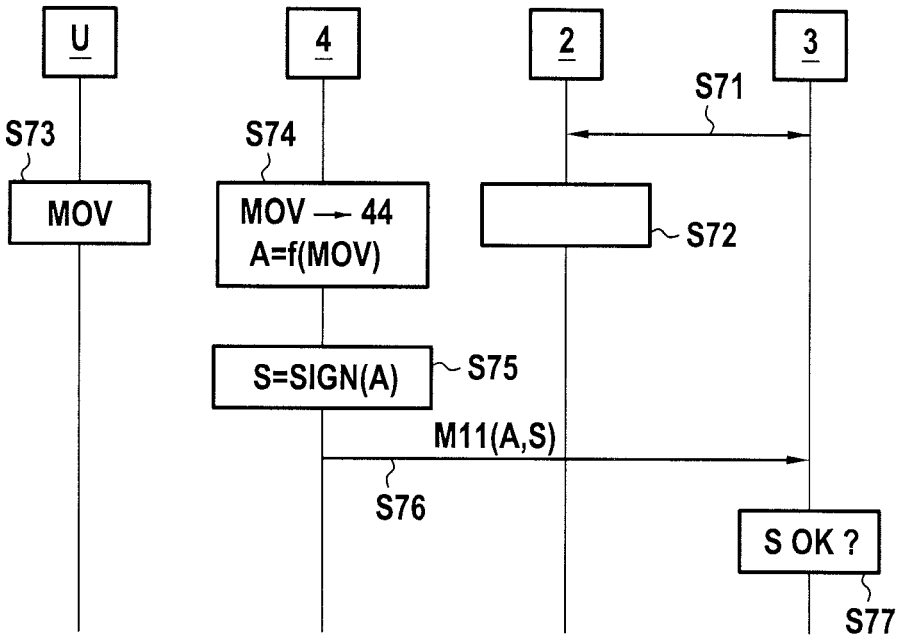

U
4
2
3
S71
S73
S74
MOV
MOV → 44
A=f(MOV)
S72
S=SIGN(A)
S75
M11(A,S)
S76
S OK ?
S77

FIG.6

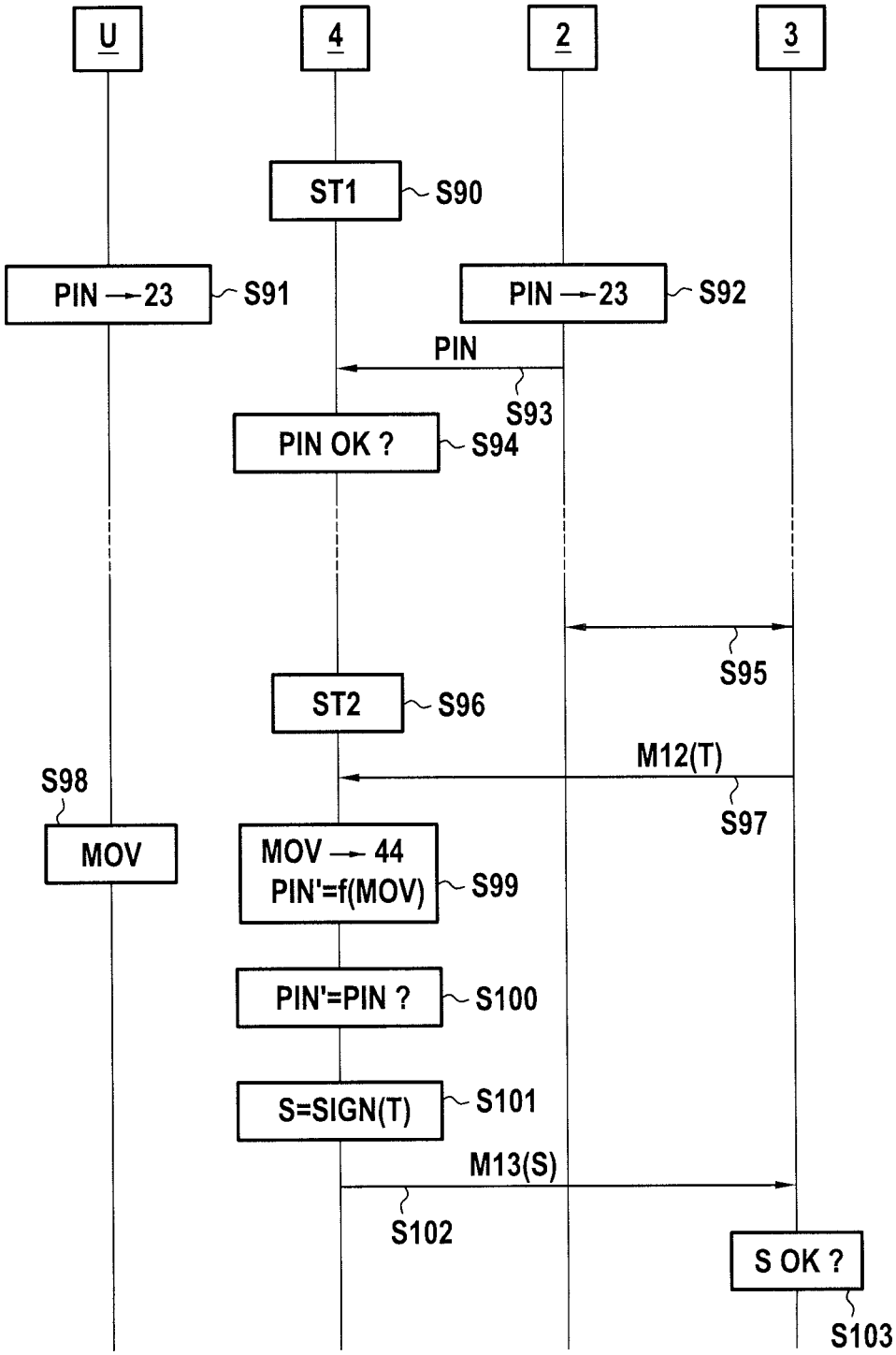

U
4
2
3
ST1
S90
PIN → 23
S91
PIN → 23
S92
PIN
S93
PIN OK ?
S94
S95
ST2
S96
M12(T)
S97
S98
MOV
MOV → 44
PIN'=f(MOV)
S99
PIN'=PIN ?
S100
S=SIGN(T)
S101
M13(S)
S102
S OK ?
S103

FIG.7

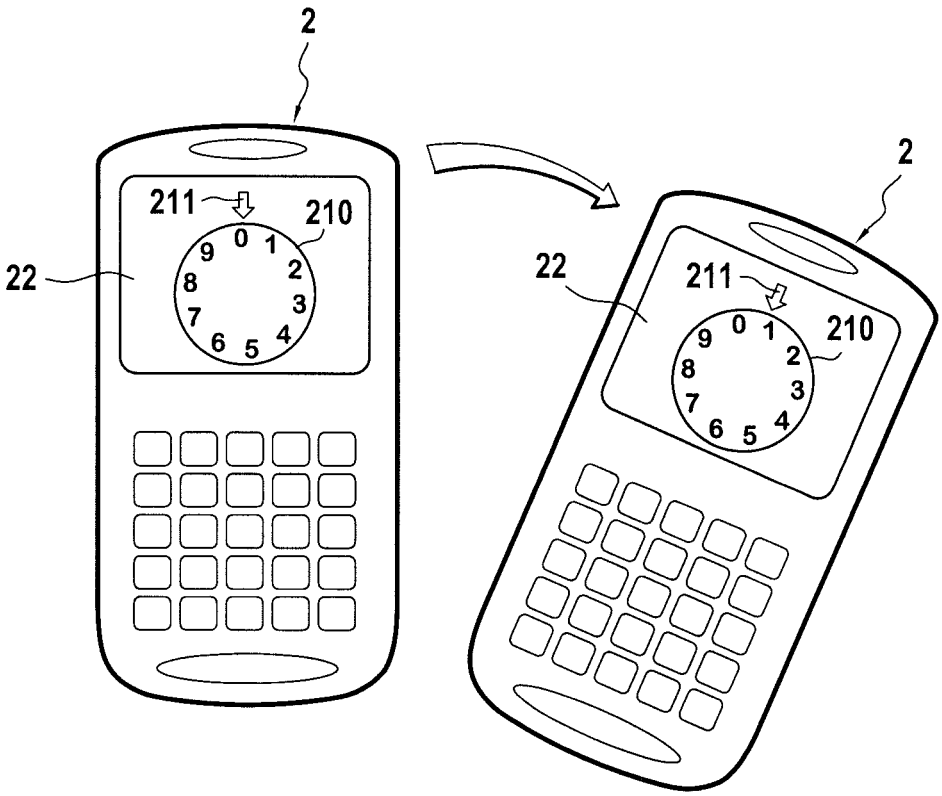


FIG.8

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 764818
FR 1251593

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	WO 2011/066381 A2 (VISA INT SERVICE ASS [US]; FAITH PATRICK [US]; CARLSON MARK [US]; HAMM) 3 juin 2011 (2011-06-03) * le document en entier * -----	1-15	G06K19/07 G06Q20/00
X	KR 2006 0135340 A (PANTECH CO LTD [KR]) 29 décembre 2006 (2006-12-29) * abrégé * -----	1-15	
X	KR 2007 0045765 A (LG ELECTRONICS INC [KR]) 2 mai 2007 (2007-05-02) * abrégé * -----	1-15	
E	US 8 255 323 B1 (CASEY BRANDON J [US] ET AL) 28 août 2012 (2012-08-28) * le document en entier * -----	1-15	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC) G06F G06Q

Date d'achèvement de la recherche	Examinateur
22 octobre 2012	Guenov, Mihail

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 1251593 FA 764818

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 22-10-2012
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
WO 2011066381 A2	03-06-2011	AU 2010324763 A1	14-06-2012
		CA 2781713 A1	03-06-2011
		US 2011187505 A1	04-08-2011
		US 2011187642 A1	04-08-2011
		US 2011189981 A1	04-08-2011
		US 2011191237 A1	04-08-2011
		WO 2011066381 A2	03-06-2011
		WO 2011066387 A2	03-06-2011
		WO 2011066395 A2	03-06-2011
		WO 2011066397 A2	03-06-2011
KR 20060135340 A	29-12-2006	AUCUN	
KR 20070045765 A	02-05-2007	AUCUN	
US 8255323 B1	28-08-2012	AUCUN	

EPO FORM P0465