

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
14 octobre 2010 (14.10.2010)

PCT

(10) Numéro de publication internationale
WO 2010/116109 A1

(51) Classification internationale des brevets :
H04L 9/32 (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2010/050693

(22) Date de dépôt international :
9 avril 2010 (09.04.2010)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0952393 10 avril 2009 (10.04.2009) FR

(71) Déposant (pour tous les États désignés sauf US) :
LYNKWARE [FR/FR]; 5, rue des Sources, F-77700
Magny Le Hongre (FR).

(72) Inventeur; et

(75) Inventeur/Déposant (pour US seulement) : PANZA,
Mauro [FR/FR]; 5, rue des Sources, F-77700 Magny Le
Hongre (FR).

(74) Mandataires : HASSINE, Albert et al.; Cabinet
Plasseraud, 52 rue de la Victoire, F-75440 Paris Cedex 09
(FR).

(81) États désignés (sauf indication contraire, pour tout titre
de protection nationale disponible) : AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ,
CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO,
DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP,
KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD,
ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI,
NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD,
SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR,
TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés (sauf indication contraire, pour tout titre
de protection régionale disponible) : ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG,
ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ,
TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE,
ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM,
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

— relative à la qualité d'inventeur (règle 4.17.iv))

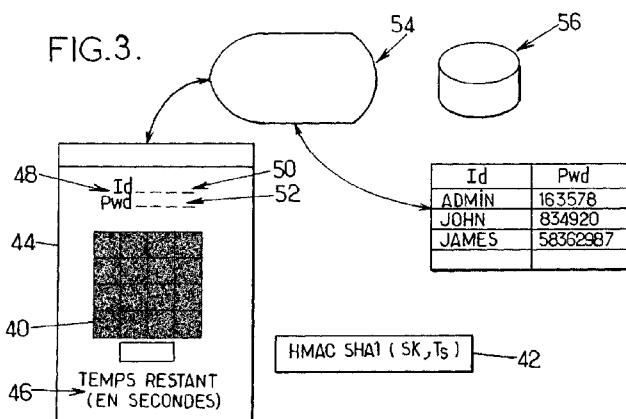
Publiée :

— avec rapport de recherche internationale (Art. 21(3))

[Suite sur la page suivante]

(54) Title : METHOD OF AUTHENTICATION AT A SERVER BY A USER OF A MOBILE APPARATUS

(54) Titre : PROCÉDÉ D'AUTHENTIFICATION AUPRÈS D'UN SERVEUR PAR UN UTILISATEUR D'UN APPAREIL
MOBILE



(57) Abstract : The invention relates to a method of authentication of a user possessing a mobile apparatus at a server, comprising: • reception (20) by the server of an authentication application request; • dispatching (22) in response by the server of an image in the form of a matrix of pixels containing an encrypted code in the pixels, the code comprising at least one time stamp value; • reception (24) of the image by the mobile apparatus and extraction (26) by the latter of the code; • generation (28) by the mobile apparatus of a single-use password based at least on the code and a secret code held by the user; • reception (30) by the server of the single-use password; and • validation (32) of the password if the latter has at least been received within a predetermined span with respect to the time stamp value, complies with the code and corresponds at least to the user authenticating himself.

(57) Abrégé : L'invention concerne un procédé d'authentification d'un utilisateur possédant un appareil mobile auprès d'un serveur, comprenant : • réception (20) par le serveur d'une requête de demande d'authentification; • envoi (22) en réponse par le serveur d'une image sous forme d'une matrice

[Suite sur la page suivante]



-
- avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues (règle 48.2.h))

de pixels contenant un code chiffré dans les pixels, le code comportant au moins une valeur d'estampille temporelle; • réception (24) de l'image par l'appareil mobile et extraction (26) par celui-ci du code; • génération (28) par l'appareil mobile d'un mot de passe à usage unique basé au moins sur le code et un code secret détenu par l'utilisateur; • réception (30) par le serveur du mot de passe à usage unique; et • validation (32) du mot de passe si celui-ci a au moins été reçu dans un délai prédéterminé par rapport à la valeur d'estampille temporelle, est conforme au code et correspond au moins à l'utilisateur s'authentifiant.

PROCEDE D'AUTHENTIFICATION AUPRES D'UN SERVEUR PAR UN UTILISATEUR D'UN APPAREIL MOBILE.

La présente invention concerne un procédé d'authentification d'un utilisateur auprès d'un serveur, l'utilisateur étant en possession d'un appareil mobile. Elle concerne également un appareil mobile et un serveur ainsi que
5 les produits programmes d'ordinateur fonctionnant sur ceux-ci et mettant en œuvre le procédé.

Les processus classiques de sécurisation des accès aux réseaux (réseau d'entreprise, Internet, etc.) consistent à valider l'identité d'un utilisateur en utilisant un identifiant et un mot de passe. Cette identification est
10 saisie sur le terminal utilisateur, ordinateur ou autre appareil mobile (téléphone portable, PDA...) puis circule sur les réseaux privés et/ou publics de communication jusqu'au système d'information qui autorise ou refuse l'accès.

Cette authentification classique a rapidement montré ses limites. Une
15 faiblesse réside notamment dans la facilité avec laquelle elle peut être contournée :

- mot de passe recopié sur un papier,
- mot de passe trivial choisi par les utilisateurs,
- mot de passe (et parfois identifiant) identique(s) pour tous les
20 services.

De plus, différentes techniques sont très répandues et en constante évolution pour récupérer ces deux informations :

- augmentation du nombre de courriels d'hameçonnage (en anglais « phishing ») qui contiennent des faux liens hypertextes pour, par
25 exemple, orienter les clients des banques vers de faux sites web bancaires.
- Avec les "renifleurs" de frappe (en anglais « keylogger »), chevaux de Troie et autres logiciels espions implantés subrepticement dans l'ordinateur de la victime, les autorisations utilisateur sensibles sont
30 recueillies et transmises aux fraudeurs.

La progression rapide de l'implantation des points d'accès « publics » utilisant les communications sans fil (cybercafés, gares, hôtels, aéroports, etc.) multiplie encore les risques d'usurpation d'identités des utilisateurs et ce d'autant plus que le personnel des entreprises est désormais mobile, avec un grand nombre d'employés qui ont un accès au réseau d'entreprise à partir de ces lieux ou de leurs foyers, en mettant en danger les données à caractère confidentiel.

Les faiblesses de ces processus classiques ont conduit à la mise au point de procédés d'authentification renforcés, qui font appel à des solutions logicielles et/ou matérielles.

Ces procédés renforcés utilisent un protocole d'échange de données entre un serveur de sécurité et l'utilisateur, protocole selon lequel un nouveau mot de passe à usage unique (en anglais « One Time Password » ou OTP) est généré pour une durée d'usage limitée, à chaque fois qu'un utilisateur est authentifié. Il est alors impossible de réutiliser ce même mot de passe lors d'une authentification ultérieure.

La technologie utilisée fait appel à un changement dynamique de mots de passe pour chaque session d'authentification. Elle permet l'authentification de l'utilisateur, car le mot de passe généré correspond au seul utilisateur qui a un périphérique physique qui génère le mot de passe.

La technologie est basée sur une clé secrète qui n'existe que dans deux endroits : sur le périphérique physique de l'utilisateur et sur le serveur de sécurité. Cette clé secrète ne peut être capturée car elle ne circule jamais entre le serveur de sécurité et l'utilisateur.

Cette clé secrète est utilisée pour calculer les mots de passe à utiliser pour authentifier l'utilisateur en cas de besoin. Le calcul se fait sur la base du temps (A) et/ou d'un événement (B) :

(A) : Cette technologie est basée sur une horloge temps réel qui est utilisée pour générer un mot de passe unique. Le dispositif matériel génère automatiquement de nouveaux mots de passe avec une fréquence déterminée (par exemple toutes les 60 secondes), en utilisant la valeur de l'horloge à l'instant « t » afin de calculer à chaque connexion un mot de passe unique.

(B) : Cette technologie se base plutôt sur un mécanisme, qui permet la génération d'un mot de passe unique pour chaque session. Le dispositif matériel génère alors un nouveau mot de passe seulement quand un événement se produit - par exemple l'utilisateur appuie sur un bouton sur sa
5 clé ou tout autre dispositif matériel. A chaque fois que l'événement a lieu un compteur est incrémenté et un algorithme bien défini va calculer un mot de passe à usage unique.

La spécificité de ces procédés est qu'ils utilisent des moyens générateurs de mot de passe chez l'utilisateur ; ces moyens sont :

- 10 • soit purement logiciels, lorsqu'une application est installée sur le terminal de l'utilisateur, on parle alors de « jetons logiciels » ; l'inconvénient de ce procédé est que l'utilisateur ne peut se connecter que sur le terminal équipé de l'application ;
- 15 • soit matériels, lorsqu'on utilise des jetons physiques tels que carte à puce, clés avec écran, clés USB, comportant un algorithme générant un nouveau mot de passe alphanumérique à intervalle de temps constant, grilles de sécurité comportant un tableau à double entrée dont les coordonnées (abscisse/ordonnée) du code de sécurité changent à chaque demande de connexion. Ces solutions
20 permettent à un utilisateur de se connecter à partir de n'importe quel terminal mais nécessitent la détention permanente d'un dispositif matériel dédié avec les risques associés (perte, détérioration...).

25 Il est par ailleurs également connu, par exemple du document de brevet FR 2 852 471 A1, des architectures d'authentification utilisant des mots de passe à usage unique. Le principe de fonctionnement de telles architectures repose sur la transmission, à un terminal, sous la forme d'une image, d'un mot de passe généré par un serveur sur demande de connexion
30 dudit terminal. L'image reçue est alors affichée par le terminal puis acquise par un dispositif générateur. Ce dernier peut alors en déduire le mot de passe.

Pour éviter notamment les attaques d'interception ou « man in the middle » en anglais, et plus particulièrement les attaques par rejeu, ou « replay attack » en anglais, visant à intercepter l'image pour s'appropriier et

utiliser le mot de passe unique à l'insu du destinataire, ces solutions, et notamment l'architecture d'authentification précédemment décrite, nécessitent le partage d'un temps commun entre le serveur et le moyen générateur de mot de passe, par exemple en mettant en œuvre des protocoles de synchronisation temporelle ou d'évènement entre l'horloge du serveur et l'horloge du moyen générateur de mot de passe de l'utilisateur. Or le partage d'un temps commun est complexe à mettre en œuvre, et peut nécessiter un certain temps, toute désynchronisation rendant le processus inopérant.

Il serait donc avantageux d'avoir un procédé d'authentification forte par l'utilisation de mot de passe à usage unique qui ne présente pas les inconvénients mentionnés ci-dessus tels que la nécessité de partager un temps commun entre le serveur et le moyen générateur de mot de passe, l'acquisition d'un dispositif spécifique, le verrouillage de l'accès sur un terminal donné et/ou la gestion de la synchronisation.

Pour résoudre un ou plusieurs des inconvénients cités précédemment, un procédé d'authentification d'un utilisateur auprès d'un serveur, ledit utilisateur étant en possession d'un appareil mobile, comprend :

- réception par le serveur d'une requête de demande d'authentification ;
- envoi en réponse par le serveur d'une image sous forme d'une matrice de pixels contenant un code chiffré dans lesdits pixels, ledit code comportant au moins une valeur d'estampille temporelle ;
- réception de l'image par l'appareil mobile et extraction par celui-ci dudit code ;
- génération par l'appareil mobile d'un mot de passe à usage unique basé au moins sur ledit code et un code secret détenu par l'utilisateur ;
- réception par le serveur dudit mot de passe à usage unique ; et
- validation dudit mot de passe si celui-ci a au moins été reçu dans un délai prédéterminé par rapport à la valeur d'estampille temporelle, et est conforme au code et correspond au moins à l'utilisateur s'authentifiant.

Le procédé d'authentification présente ainsi l'avantage d'utiliser le téléphone portable comme matériel de génération du mot de passe. L'usage de cet équipement est très largement répandu et autorise une utilisation de l'authentification forte dans des applications « grand public » qui peuvent
5 exiger un niveau élevé de sécurité d'accès (domaines bancaire, médical...).

De plus, avantageusement, l'horloge de l'appareil mobile n'a pas besoin d'être synchronisée avec le serveur car l'image contient en interne la donnée nécessaire à la limitation de validité du mot de passe.

L'image contient par exemple une signature cryptée non symétrique
10 de l'estampille temporelle et de la clef du serveur, seul le serveur contenant la limitation de validité du mot de passe.

En outre, la transmission du code comportant l'estampille temporelle permet d'augmenter significativement le niveau de sécurité du procédé, car il est par exemple possible par des procédés de hachage et/ou signature
15 connus de vérifier que le code comportant l'estampille est bien intègre et a bien été transmis par le serveur. Il est ainsi possible de détecter toutes anomalies portant sur le code, et donc simultanément sur l'entité comprenant l'estampille et les données pour générer le mot de passe unique. Il est ainsi possible de s'assurer que l'estampille n'a pas été altérée et correspond bien
20 aux données pour générer le mot de passe unique, en vérifiant le code reçu.

Des caractéristiques ou des modes de réalisation particuliers utilisables seuls ou en combinaison sont :

- l'image est envoyée par le serveur sur un écran et l'appareil mobile réceptionne cette image par l'intermédiaire d'une caméra incluse
25 dans l'appareil mobile ou bien l'image est envoyée par le serveur à l'appareil mobile via le réseau de téléphonie mobile ;
- l'image comporte un code-barres 2D contenant le code ou bien le code est inclus par un procédé de stéganographie dans l'image ;
- l'appareil mobile comportant un code d'identification de celui-ci
30 (IMEI) et/ou un code d'identification de l'utilisateur (IMSI), le mot de passe à usage unique est généré en se basant en outre sur le code d'identification de l'appareil mobile, le code d'identification de l'utilisateur ou une combinaison des deux ; et
- le code comporte en outre un identifiant du serveur.

L'utilisation des codes d'identification contenu dans l'appareil mobile tels que, par exemple, l'IMEI qui est un identifiant unique d'un téléphone mobile à la norme GSM ou 3G, ou l'IMSI qui est un identifiant contenu dans la carte SIM du téléphone et en relation avec l'abonné permet un renforcement

5 de la sécurité :

en validant que l'appareil qui a réalisé le calcul du mot de passe est identifié.

en facilitant le blocage par l'opérateur de téléphonie de l'appareil mobile perdu ou volé

10 La transmission d'une clé spécifique au serveur dans le code chiffré permet avantageusement de faire un lien entre l'appareil mobile et le serveur sans que l'appareil mobile ait à stocker une clé secrète.

Dans un deuxième aspect de l'invention, un appareil mobile comprend :

- 15
- des moyens d'acquisition d'une image comportant un code ledit code comportant au moins une valeur d'estampille temporelle ;
 - des moyens d'extraction dudit code ;
 - des moyens de saisie d'un code secret ; connectés à
 - un calculateur de mot de passe basé sur ledit code et ledit code
- 20 secret.

Selon un troisième aspect de l'invention, un serveur comporte :

- des moyens de réception d'une requête d'authentification d'un utilisateur et d'un mot de passe à usage unique ;
 - un générateur de code, ledit code comportant au moins une valeur
- 25 d'estampille temporelle ;
- un générateur d'image comportant dans ses pixels ledit code ; connecté à
 - des moyens de transmission de ladite image ;
 - des moyens de validation dudit mot de passe à usage unique
- 30 adaptés pour vérifier que ledit mot de passe a au moins été reçu dans un délai prédéterminé par rapport à la valeur d'estampille temporelle, est conforme au code et correspond au moins à l'utilisateur s'authentifiant.

Selon un quatrième aspect de l'invention, un produit programme d'ordinateur comportant des instructions de code de programme enregistrées sur un support lisible par un ordinateur de serveur, pour mettre en œuvre les étapes d'un procédé d'authentification d'un utilisateur auprès dudit serveur,

5 ledit utilisateur étant en possession d'un appareil mobile, comportant :

- réception d'une requête de demande d'authentification ;
- envoi en réponse d'une image sous forme d'une matrice de pixels contenant un code chiffré dans lesdits pixels, ledit code comportant au moins une valeur d'estampille temporelle ;
- 10 • réception d'un mot de passe à usage unique basé au moins sur ledit code et un code secret détenu par l'utilisateur ; et
- validation dudit mot de passe si celui-ci a au moins été reçu dans un délai prédéterminé par rapport à la valeur d'estampille temporelle, est conforme au code et correspond au moins à
- 15 l'utilisateur s'authentifiant.

L'invention sera mieux comprise à la lecture de la description qui suit, faite uniquement à titre d'exemple, et en référence aux figures en annexe dans lesquelles :

- la figure 1 est une vue schématique d'un système pour mettre en œuvre un mode de réalisation de l'invention ;
- 20 - la figure 2 est un ordinogramme d'un procédé d'authentification selon un mode de réalisation de l'invention ;
- la figure 3 est une vue schématique de fonctionnement d'une authentification sur un serveur mettant en œuvre le procédé de la figure 2 ;
- 25 - la figure 4 est une vue schématique d'exemples d'écrans de visualisation générés par l'authentification de la figure 3 ;
- la figure 5 est une vue schématique de fonctionnement d'une reconnaissance d'image sur un terminal mobile durant l'exécution du procédé de la figure 2 ;
- 30 - la figure 6 est une vue schématique de l'appareil mobile de la figure 1 ;
- la figure 7 est une vue schématique du serveur de la figure 1 ;

- la figure 8 est une vue schématique de transmission d'une image codée dans une variante de mode de réalisation ; et
- la figure 9 est une vue schématique d'écrans d'un terminal mobile dans une autre variante de mode de réalisation.

5 En référence à la figure 1, l'authentification par mot de passe à usage unique décrite ci-après met en œuvre un serveur 1 connecté à un terminal utilisateur 3 par lequel un utilisateur 5 souhaite accéder à un service contrôlé par le serveur 1, et un appareil mobile 7 possédé par l'utilisateur 5.

10 L'appareil mobile 7 est typiquement un téléphone mobile possédant un clavier 9 ou un écran tactile, un écran de visualisation 11 et une caméra 13 de prise de vue.

 Le serveur 1 et l'appareil mobile 7 possèdent des moyens programmables de calcul , non représentés, ainsi que des moyens de stockage de données et de programme.

15 L'authentification se déroule alors de la façon suivante, figure 2 :

- réception, étape 20, par le serveur 1 d'une requête de demande d'authentification provenant du terminal utilisateur 3 ;
- envoi, étape 22, en réponse par le serveur 1 d'une image sous forme d'une matrice de pixels contenant un code chiffré dans les pixels de l'image, le code comportant au moins une valeur de signature de l'estampille temporelle, aussi appelée valeur d'horodatage ;
- 20 • réception de l'image sur le dispositif d'affichage du terminal utilisateur 3 ;
- 25 • lecture, étape 24, de l'image par la caméra de l'appareil mobile et extraction, étape 26, par celui-ci du code ;
- génération, étape 28, par l'appareil mobile d'un mot de passe à usage unique basé au moins sur le code et un code secret détenu par l'utilisateur ;
- 30 • saisie sur le terminal utilisateur du mot de passe à usage unique, au moyen d'un clavier ou de tout autre dispositif de saisie ;
- réception, étape 30, par le serveur du mot de passe à usage unique ; et

- validation, étape 32, du mot de passe si celui-ci a au moins été reçu dans un délai prédéterminé par rapport à la valeur d'estampille temporelle, est conforme au code et correspond au moins à l'utilisateur s'authentifiant.

5 Ces étapes vont maintenant être décrites plus en détail dans le cadre d'un mode de réalisation utilisant un code-barres 2D comme image support du code.

L'appareil mobile 7 comporte une application mobile qui peut s'installer sur les différents téléphones portables du marché et capable de
10 faire du traitement d'image. L'application est ainsi disponible sur différentes plateformes logicielles utilisées par les fabricants de téléphone portable telles que, par exemple, J2ME, WM, Symbian, MacOS, Androïd, RIM Os et BREW.

L'application mobile pour générer le mot de passe unique est incluse dans un lecteur d'images code-barres 2D et se sert d'une balise contenue
15 dans le code-barres pour lancer une interface de génération du mot de passe à usage unique.

L'application mobile réalise les différentes étapes suivantes :

- prise de vue de l'image du code-barres 2D ;
- décodage du code barre ;
- 20 • détection de la balise dans la donnée résultant du décodage ;
- interprétation de la donnée en fonction de la balise ;
- affichage d'une interface de saisie du mot de passe ;
- génération du mot de passe à usage unique en utilisant le mot de passe et la donnée du code-barres ;
- 25 • affichage du mot de passe sur l'écran du mobile ;

L'application mobile peut être installée sur un téléphone mobile en positionnant sur un serveur WAP une page avec le lien vers le fichier à télécharger, spécifique à chaque téléphone. Une autre solution consiste à charger et installer directement l'application via le câble USB ou via Bluetooth.

30 Sur le serveur, figure 3, une application serveur, par exemple écrite en PHP, est capable de générer des codes-barres 2D chiffrés 40. Classiquement, il existe deux types de code-barres 2D largement utilisés : le Datamatrix ou le QR code. Le Datamatrix a l'avantage d'être facile à lire et de

compresser aisément des données. Le QR code à l'avantage de garantir la lecture des codes sur les mobiles asiatiques.

Le code-barres 2D 40 contient un code 42 qui est une valeur de hachage d'une clé secrète SK du serveur et d'une donnée d'estampille temporelle Ts. Cette dernière est, par exemple, sur un serveur Unix/Linux le temps Epoch de l'horloge du système. Pour rappel, le temps Epoch correspond au nombre de millisecondes écoulées depuis le 1^{er} janvier 1970. Le hachage est réalisé par une des nombreuses fonctions de hachage connues telles que MD5, SHA-1 ou HMAC. La donnée d'estampille temporelle Ts est générée, par exemple, en lisant l'heure courante du serveur sensiblement à l'instant où le code 42 est produit, et en associant l'heure courante lue à la valeur de la donnée de l'estampille.

Le serveur détermine également le délai prédéterminé par rapport à la valeur d'estampille temporelle, ou durée de validité. La durée de validité est par exemple une durée à partir de l'heure correspondant à la donnée temporelle Ts, définissant une période pendant laquelle l'utilisateur peut s'authentifier en utilisant le mot de passe correspondant au code 42.

Ainsi, sur réception d'une requête d'authentification, le serveur présente à l'utilisateur une fenêtre 44 d'autorisation d'accès comportant le code-barres 2D, un compte à rebours 46 indiquant la durée de validité du code-barres 2D et un formulaire 48 comportant un champ 50 d'identification Id de l'utilisateur et un champ 52 de saisie du mot de passe à usage unique Pwd. La durée de validité du code-barres 2D du compte à rebours 46 peut être obtenue en utilisant une durée par défaut, fixée par configuration par exemple, égale à la durée de validité du serveur.

Le serveur contient également une application 54 capable de vérifier les mots de passe à usage unique et une base de données 56 pour archiver les données d'authentification des utilisateurs.

L'interaction avec la base de données est réalisée par des requêtes SQL standard permettant de maintenir des applications indépendantes du type de base de données utilisée. L'utilisation des procédures stockées peut augmenter le niveau de sécurité mais au détriment d'un lien de l'application à une base de données spécifique.

L'application 54, à réception des champs d'identification et de mot de passe du formulaire 48 vérifie :

- que le mot de passe correspond au code contenu dans le code-barres 2D ;
- 5 • que la réception a eu lieu à l'intérieur de la fenêtre temporelle de validité ;
- que l'identifiant et le mot de passe correspondent indiquant ainsi que l'utilisateur a utilisé son code secret personnel.

Cette validation est réalisée typiquement en réalisant les mêmes
10 calculs que le terminal mobile en se basant sur les données contenues dans la base de données 56, identifiant et code secret de l'utilisateur, et le code chiffré dans le code-barres 2D.

Si, pour une raison quelconque, l'utilisateur ne rentre pas les données dans la fenêtre temporelle de validité prévue, figure 4, la fenêtre d'autorisation
15 44 est remplacée par une fenêtre 60 indiquant que la durée de validité a expirée et qu'un nouveau code va être généré.

Au niveau de l'utilisateur, figure 5, celui-ci, via la caméra intégrée dans son téléphone, va lire 70 le code 2D généré et transmis par le serveur et qui est affiché sur l'écran de son ordinateur. L'application mobile lui présente
20 alors un écran 72 indiquant qu'elle a bien acquis le code. Elle lui présente ensuite un écran de saisie 74 lui permettant de saisir son code secret personnel. Au vu des claviers ou des écrans tactiles des téléphones actuels, ce code secret est composé d'une série de chiffres mais cela n'est pas limitatif dans la mesure où les nouvelles générations de téléphone mobile offrent des
25 claviers ou des écrans tactiles de plus en plus ergonomiques et mettant à disposition un jeu complet de caractères alphanumériques. L'application mobile affiche alors sur un écran 76 le mot de passe à usage unique généré selon un algorithme se basant sur les paramètres suivants :

- les données chiffrées dans le code-barres 2D à savoir la clé unique
30 du serveur SK et la donnée d'estampille temporelle Ts ;
- le code secret fourni par l'utilisateur qui est également sauvegardé dans la base de données 56 du serveur ;

Ainsi, l'appareil mobile comprend, figure 6 :

- des moyens d'acquisition d'une image comportant un code, tels que la caméra 13 ;
- des moyens d'extraction 60 du code ;
- des moyens de saisie 9 d'un code secret ; connectés à
- 5 • un calculateur 62 de mot de passe basé sur le code et le code secret.

Et le serveur 1 comporte :

- des moyens de réception 70 d'une requête d'authentification d'un utilisateur et d'un mot de passe à usage unique ;
- 10 • un générateur de code 72, le code comportant au moins une valeur d'estampille temporelle ;
- un générateur d'image 76 comportant dans ses pixels le code ; connecté à
- des moyens 78 de transmission de l'image ;
- 15 • des moyens de validation 79 du mot de passe à usage unique adaptés pour vérifier que le mot de passe a au moins été reçu dans un délai prédéterminé par rapport à la valeur d'estampille temporelle, est conforme au code et correspond au moins à l'utilisateur s'authentifiant.

Dans une première variante, le mot de passe à usage unique est
20 généré par l'application mobile en utilisant également le numéro IMEI (« International Mobile Equipment Identity » - numéro d'identification international de l'équipement mobile) qui est également sauvegardé dans la base de données 56 du serveur. Ce numéro IMEI est un numéro unique attribué à chaque téléphone portable et est enregistré dans une base de
25 données gérée en général par les opérateurs et utilisée particulièrement pour lutter contre le vol.

L'application serveur de validation du mot de passe intègre alors également le numéro IMEI contenu dans la base de données 56 parmi les paramètres de calcul.

30 L'intégration dans le processus d'authentification du numéro IMEI du téléphone mobile minimise les risques d'usurpation d'identité en cas de perte ou de vol. En effet, les opérateurs de téléphonie mobile désactivent alors le fonctionnement de l'appareil volé ou perdu sur simple appel.

Dans une deuxième variante, le numéro IMEI peut être remplacé par le numéro IMSI (« International Mobile Subscriber Identity » - identification internationale de l'abonné mobile) qui est un numéro d'identification de l'abonné contenu dans la carte à puce intégrée au téléphone mobile, carte à
5 puce aussi appelée carte SIM (« Subscriber Identity Module » - module d'identification de l'abonné).

L'utilisation des numéros IMEI et IMSI peut être combinée de façon à renforcer encore la sécurité de l'authentification.

Dans une troisième variante, l'image d'un code-barres 2D est
10 remplacée par une image quelconque dans laquelle le code chiffré est inséré par stéganographie. Les pixels de l'image sont ainsi modifiés sans que cela soit obligatoirement visible par l'œil humain tout en étant détectables par un algorithme de reconnaissance adapté.

Dans une quatrième variante, figure 6, l'image n'est pas transmise via
15 le terminal d'authentification et une prise d'image par la caméra du téléphone mobile mais elle est envoyée directement au téléphone mobile 7 via le réseau téléphonique, par exemple sous forme d'un MMS (« Multimedia Message Service » - service de messages multimédia) ou en utilisant les possibilités d'accès à internet du téléphone mobile telles que le protocole Wap, ou via une
20 capture d'écran de l'affichage du mobile (par exemple, une capture d'écran du navigateur internet du mobile).

La figure 7 illustre une combinaison des troisième et quatrième variantes sous la forme d'une succession d'écrans du téléphone mobile 7. L'écran 80 illustre la réception d'une image contenant le code du serveur et la
25 valeur d'estampille temporelle chiffrés par stéganographie dans ses pixels. L'écran 82 correspond à la saisie du code secret de l'utilisateur, une fois que l'application installée sur le téléphone mobile 7 a déchiffré les valeurs contenues dans l'image. Et l'écran 84 correspond à l'écran d'affichage du mot de passe à usage unique à fournir au formulaire d'authentification.

30 L'invention a été illustrée et décrite en détail dans les dessins et la description précédente. Celle-ci doit être considérée comme illustrative et donnée à titre d'exemple et non comme limitant l'invention à cette seule description. De nombreuses variantes de réalisation sont possibles.

Par exemple, et en particulier, le procédé peut prévoir les techniques habituelles de gestion des échecs d'authentification telles que, par exemple, le blocage du compte après un nombre prédéterminé d'échecs consécutifs accompagné, ou non, d'une procédure de reprise/déblocage du compte.

- 5 Dans les revendications, le mot « comprenant » n'exclue pas d'autres éléments et l'article indéfini « un/une » n'exclue pas une pluralité.

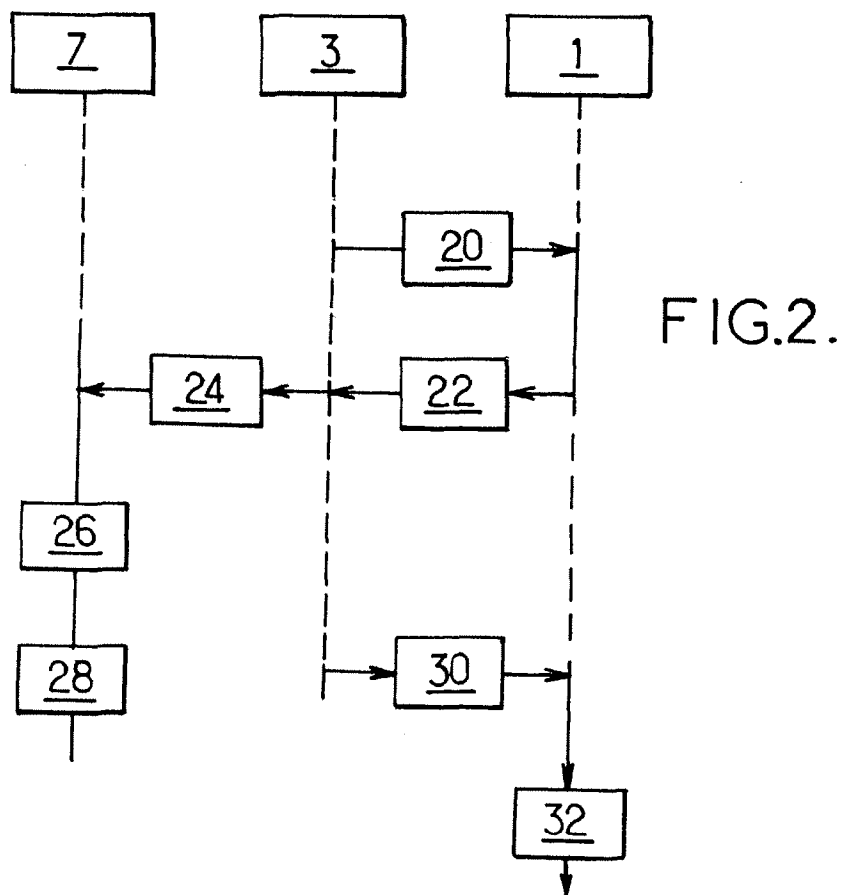
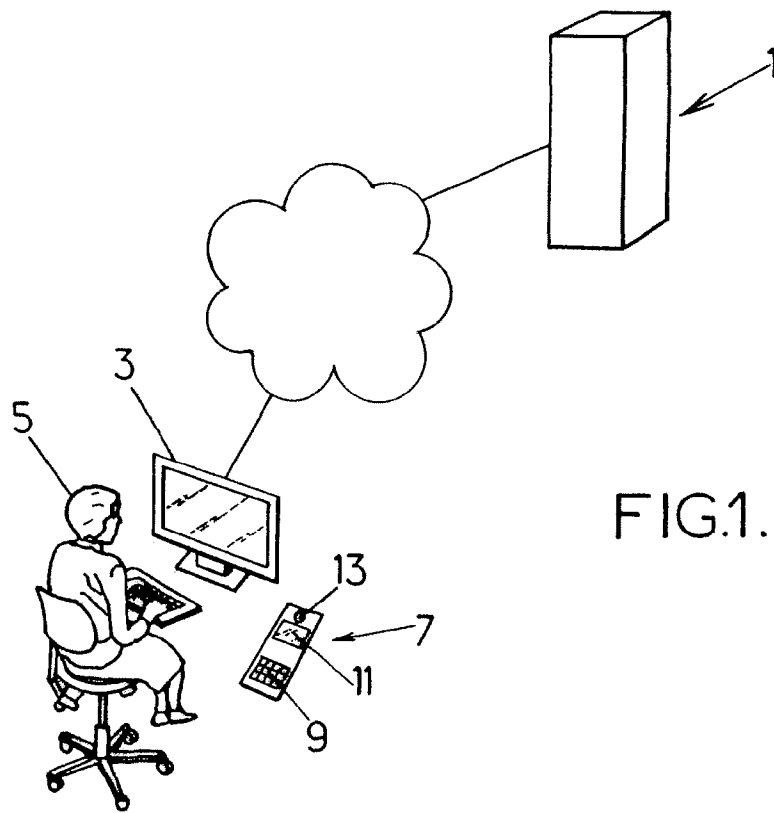
REVENDICATIONS

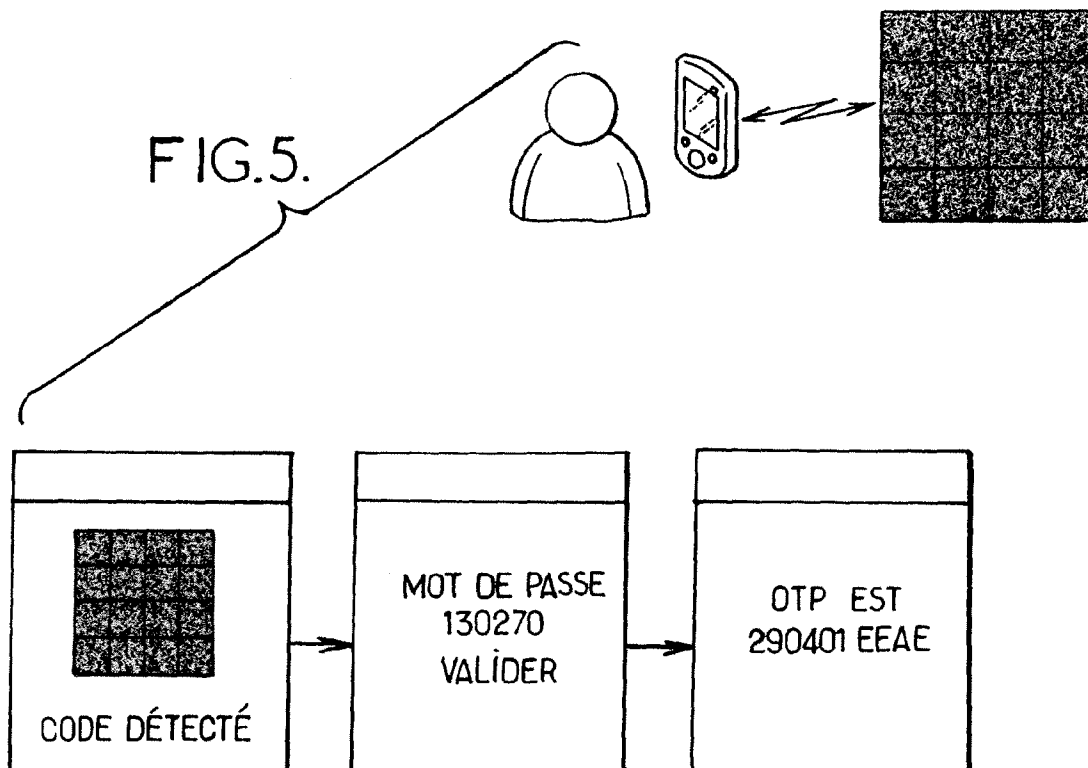
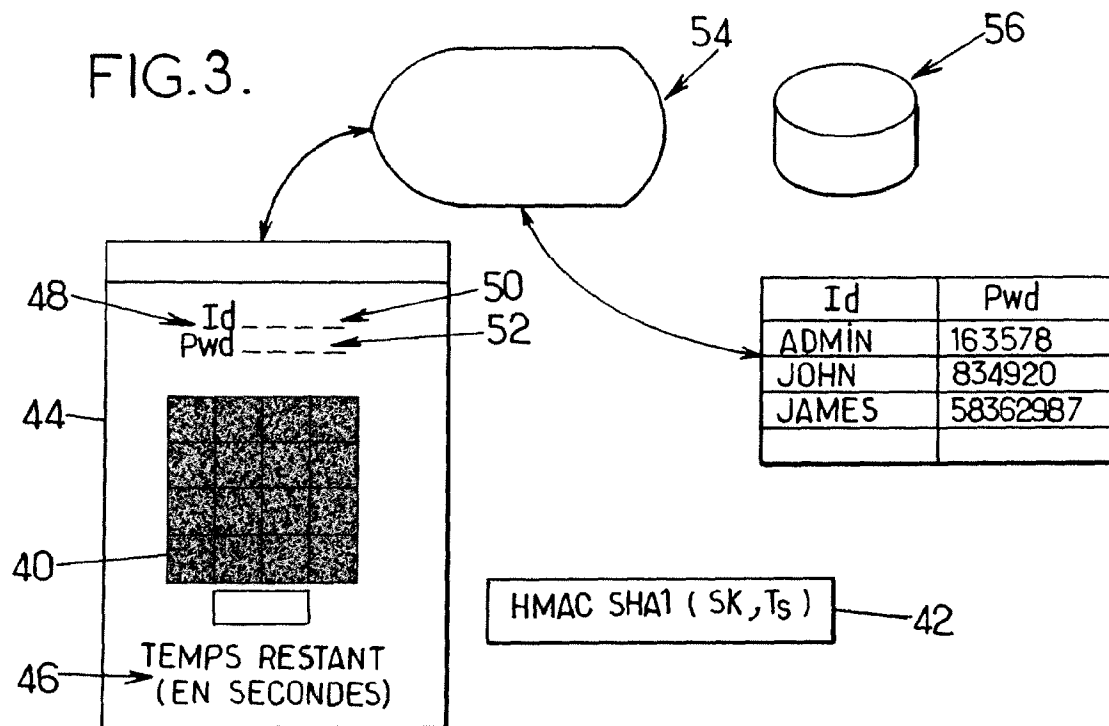
1. Procédé d'authentification d'un utilisateur auprès d'un serveur, ledit utilisateur étant en possession d'un appareil mobile, comprenant:
 - 5 • réception (20) par le serveur d'une requête de demande d'authentification ;
 - envoi (22) en réponse par le serveur d'une image sous forme d'une matrice de pixels contenant un code chiffré dans lesdits pixels, ledit code comportant au moins une valeur d'empreinte temporelle ;
 - 10 • réception (24) de l'image par l'appareil mobile et extraction (26) par celui-ci dudit code ;
 - génération (28) par l'appareil mobile d'un mot de passe à usage unique basé au moins sur ledit code et un code secret détenu par l'utilisateur ;
 - réception (30) par le serveur dudit mot de passe à usage unique ; et
 - 15 • validation (32) dudit mot de passe si celui-ci a au moins été reçu dans un délai prédéterminé par rapport à la valeur d'empreinte temporelle, est conforme au code et correspond au moins à l'utilisateur s'authentifiant.
2. Procédé selon la revendication 1, caractérisé en ce que l'image est
20 envoyée par le serveur sur un écran et l'appareil mobile réceptionne cette image par l'intermédiaire d'une caméra incluse dans l'appareil mobile.
3. Procédé selon la revendication 1, caractérisé en ce que l'image est
25 envoyée par le serveur à l'appareil mobile via le réseau de téléphonie mobile.
4. Procédé selon les revendications 2 ou 3, caractérisé en ce que l'image comporte un code-barres 2D contenant le code.
- 30 5. Procédé selon les revendications 2 ou 3, caractérisé en ce que le code est inclus par un procédé de stéganographie dans l'image.

6. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que l'appareil mobile comportant un code d'identification de celui-ci (IMEI) et/ou un code d'identification de l'utilisateur (IMSI), le mot de passe à usage unique est généré en se basant en outre sur le code d'identification de l'appareil mobile, le code d'identification de l'utilisateur ou une combinaison des deux.
7. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que ledit code comporte en outre un identifiant dudit serveur.
8. Appareil mobile comprenant :
- des moyens d'acquisition (13) d'une image comportant un code, ledit code comportant au moins une valeur d'estampille temporelle ;
 - des moyens d'extraction (60) dudit code ;
 - des moyens de saisie (9) d'un code secret ; connectés à
 - un calculateur (62) de mot de passe basé sur ledit code et ledit code secret.
9. Appareil mobile selon la revendication 8, caractérisé en ce qu'il comporte en outre une mémoire de stockage d'un code d'identification dudit appareil mobile (IMEI) et/ou un code d'identification de l'utilisateur (IMSI), ledit calculateur étant adapté pour calculer en outre le mot de passe à partir dudit code d'identification de l'appareil mobile, dudit code d'identification de l'utilisateur ou d'une combinaison des deux.
10. Serveur comportant :
- des moyens de réception (70) d'une requête d'authentification d'un utilisateur et d'un mot de passe à usage unique ;
 - un générateur de code (72), ledit code comportant au moins une valeur d'estampille temporelle ;
 - un générateur d'image (76) comportant dans ses pixels ledit code ; connecté à

- des moyens (78) de transmission de ladite image ;
- des moyens de validation (79) dudit mot de passe à usage unique adaptés pour vérifier que ledit mot de passe a au moins été reçu dans un délai prédéterminé par rapport à la valeur d'estampille temporelle, est conforme au code et correspond au moins à l'utilisateur s'authentifiant.

11. Produit programme d'ordinateur comportant des instructions de code de programme enregistrées sur un support lisible par un calculateur de serveur, pour mettre en œuvre les étapes d'un procédé d'authentification d'un utilisateur auprès dudit serveur, ledit utilisateur étant en possession d'un appareil mobile, comportant :
- réception d'une requête de demande d'authentification ;
 - envoi en réponse d'une image sous forme d'une matrice de pixels contenant un code chiffré dans lesdits pixels, ledit code comportant au moins une valeur d'estampille temporelle ;
 - réception d'un mot de passe à usage unique basé au moins sur ledit code et un code secret détenu par l'utilisateur ; et
 - validation dudit mot de passe si celui-ci a au moins été reçu dans un délai prédéterminé par rapport à la valeur d'estampille temporelle, est conforme au code et correspond au moins à l'utilisateur s'authentifiant.





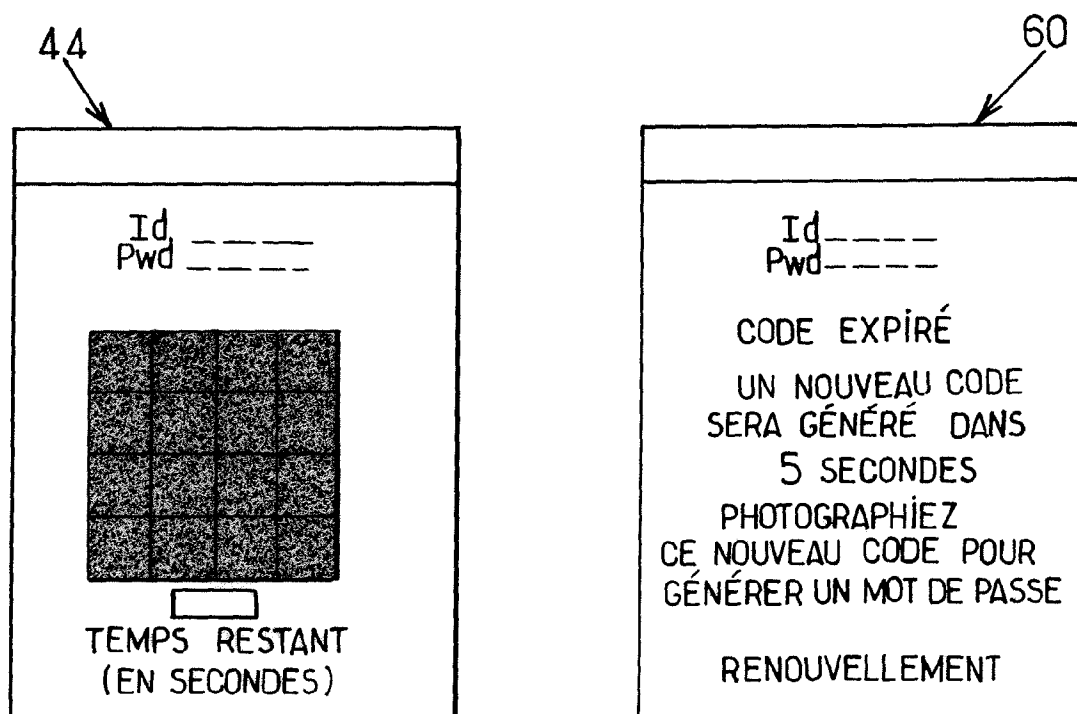


FIG.4.

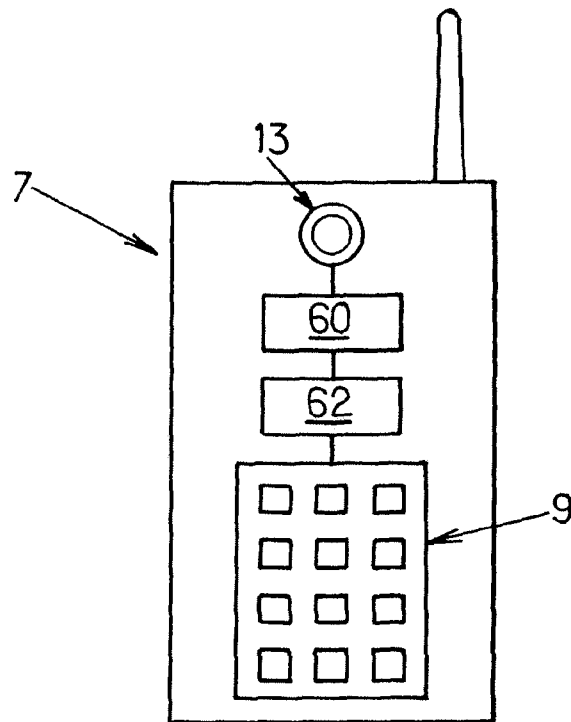


FIG. 6.

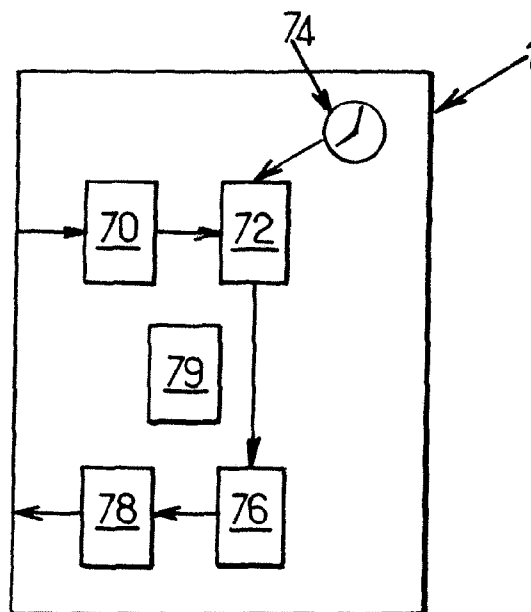


FIG. 7.

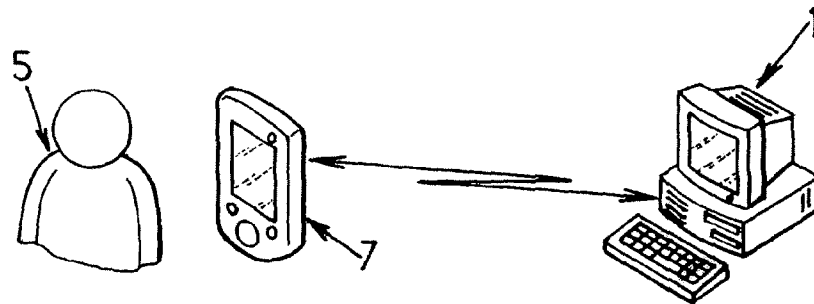


FIG.8.

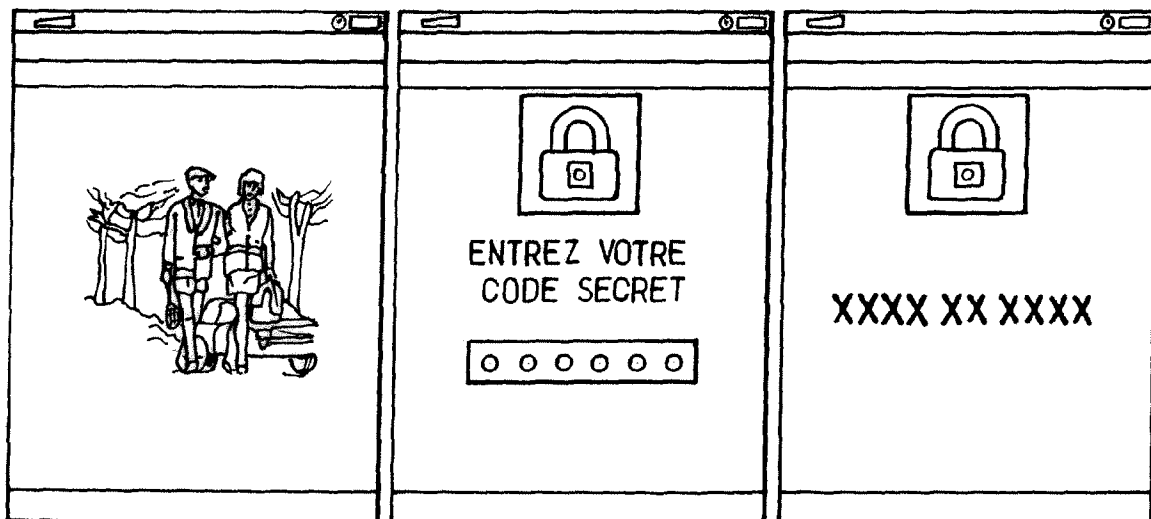


FIG.9.

INTERNATIONAL SEARCH REPORT

International application No

PCT/FR2010/050693

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L9/32

ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the International search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	FR 2 852 471 A1 (FRANCE TELECOM [FR]) 17 September 2004 (2004-09-17) the whole document	1-11
Y	US 2006/048212 A1 (TSURUOKA YUKIO [JP] ET AL) 2 March 2006 (2006-03-02) paragraphs [0044], [0 79]	1-11
Y	US 2007/174198 A1 (KASAHARA AKIHIRO [JP] ET AL) 26 July 2007 (2007-07-26) paragraph [0021] - paragraph [0073] figures 1-6	6, 7, 9

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the International filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

3 August 2010

Date of mailing of the international search report

10/08/2010

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Bec, Thierry

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/FR2010/050693

Patent document cited in search report		Publication date		Patent family member(s)	Publication date
FR 2852471	A1	17-09-2004	WO	2004082354 A2	30-09-2004
US 2006048212	A1	02-03-2006	CN	1701561 A	23-11-2005
			EP	1646177 A1	12-04-2006
			WO	2005011192 A1	03-02-2005
			JP	4425859 B2	03-03-2010
US 2007174198	A1	26-07-2007	JP	2006048464 A	16-02-2006
			WO	2006013684 A1	09-02-2006

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/FR2010/050693

A. CLASSEMENT DE L'OBJET DE LA DEMANDE

INV. H04L9/32

ADD.

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)

EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	FR 2 852 471 A1 (FRANCE TELECOM [FR]) 17 septembre 2004 (2004-09-17) le document en entier	1-11
Y	US 2006/048212 A1 (TSURUOKA YUKIO [JP] ET AL) 2 mars 2006 (2006-03-02) alinéas [0044], [0 79]	1-11
Y	US 2007/174198 A1 (KASAHARA AKIHIRO [JP] ET AL) 26 juillet 2007 (2007-07-26) alinéa [0021] - alinéa [0073] figures 1-6	6,7,9

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

3 août 2010

Date d'expédition du présent rapport de recherche internationale

10/08/2010

Nom et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Bec, Thierry

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°

PCT/FR2010/050693

Document brevet cité au rapport de recherche		Date de publication		Membre(s) de la famille de brevet(s)	Date de publication
FR 2852471	A1	17-09-2004	WO	2004082354 A2	30-09-2004
US 2006048212	A1	02-03-2006	CN	1701561 A	23-11-2005
			EP	1646177 A1	12-04-2006
			WO	2005011192 A1	03-02-2005
			JP	4425859 B2	03-03-2010
US 2007174198	A1	26-07-2007	JP	2006048464 A	16-02-2006
			WO	2006013684 A1	09-02-2006