(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
12 mars 2015 (12.03.2015)

WIPO | PCT

(10) Numéro de publication internationale
WO 2015/033061 A1

(51) Classification internationale des brevets :
G06Q 20/32 (2012.01) *G06Q 20/38* (2012.01)

(21) Numéro de la demande internationale :
PCT/FR2014/052176

(22) Date de dépôt international :
3 septembre 2014 (03.09.2014)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
13.58428 3 septembre 2013 (03.09.2013) FR
14.56157 30 juin 2014 (30.06.2014) FR

(72) Inventeur; et
(71) Déposant : **RUIZ, Emmanuel** [FR/FR]; 848 chemin du Carreyrat, F-82000 Montauban (FR).

(74) Mandataire : **CABINET BARRE LAFORGUE & ASSOCIÉS**; 35 rue Lancefoc, F-31000 Toulouse (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, BN, 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, IR, IS, JP, KE, KG, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, 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, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Publiée :

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

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

(54) **Title** : METHOD FOR AUTHENTICATING A TRANSACTION

(54) **Titre** : PROCÉDÉ D'AUTHENTIFICATION DE TRANSACTION

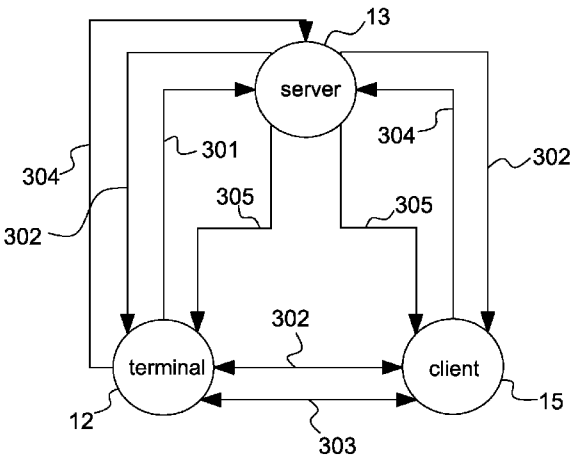

Fig.2

(57) **Abstract** : The invention relates to a method for authenticating a transaction between two users of said method, comprising the following steps: a one-time password is generated by an authentication server (13) at the request of one of the two users; the one-time password is split into at least two segments sent to at least one (12) of the mobile terminals; the sonic and/or ultrasonic messages corresponding to the one-time password segments are exchanged sonically and/or ultrasonically between the mobile terminals (12, 15); and the authentication server (13) receives the sonic and/or ultrasonic messages, decodes same in order to extract the segments therefrom, and compares the message once reconstituted with said one-time password for validation.

(57) **Abrégé** : L'invention vise un procédé d'authentification de transaction entre deux utilisateurs dudit procédé, comportant des étapes dans lesquelles un mot de passe à usage unique est généré par un serveur d'authentification (13) à la demande d'un des deux utilisateurs. Le mot de passe à usage unique est coupé en au moins deux segments envoyés à l'un (12) au moins des terminaux mobiles, les messages soniques et/ou ultrasoniques correspondant aux segments de mot de passe à usage unique sont échangés par voie sonique et/ou ultrasonique entre les terminaux mobiles (12, 15), le serveur d'authentification (13) reçoit les messages soniques et/ou ultrasoniques, les décode pour en extraire les segments, et compare le message une fois reconstitué avec ledit mot de passe à usage unique pour validation.

WO 2015/033061 A1

PROCÉDÉ D'AUTHENTIFICATION DE TRANSACTION

La présente invention vise un procédé d'authentification entre deux utilisateurs pour procédé de transfert de données. Elle vise plus précisément un procédé d'authentification dite forte, sans contact en champ proche, notamment pour procédé de paiement à distance.

Elle relève du domaine des procédés de transmission de données de manière sécurisée.

Dans tout le texte, le terme « serveur » désigne de façon générale la fonction informatique consistant à mettre des données et/ou des ressources informatiques à disposition d'humains et/ou de machines, ces ressources étant accessibles par l'intermédiaire d'au moins un réseau de communication (réseau de télécommunication et/ou réseau informatique). Ainsi, un serveur peut être matériellement constitué de tout système informatique, y compris un unique ordinateur ou une pluralité d'ordinateurs reliés selon un réseau ou une grille. Le terme « mobile » et ses dérivés appliqués à un terminal désigne le fait que ce dernier est portatif et adapté pour pouvoir fonctionner sans fil de liaison avec un environnement externe, notamment pour communiquer avec un réseau. Le terme « utilisateur » désigne un humain utilisant au moins pour partie un procédé selon l'invention.

En outre, le terme « transaction » désigne de façon générale toute opération pouvant intervenir entre des utilisateurs soumise au moins à une authentification par au moins un serveur sécurisé. Il peut en particulier s'agir d'une transaction financière (notamment transaction bancaire telle qu'un virement) ; d'une transaction commerciale (notamment transaction de paiement lors d'un achat) ; d'une transaction juridique ou contractuelle (preuve d'un accord donné sur une convention, par exemple lors d'un accès à un réseau ou lors du téléchargement ou de l'utilisation d'un logiciel) ; d'une transaction technique (par exemple configuration d'un accès à un réseau (par exemple de télécommunications et/ou informatique) pour un utilisateur identifié).

Par ailleurs, les termes « audio » et « acoustique» se réfèrent de façon générale aux sons et aux ondes sonores, c'est-à-dire aussi bien aux sons audibles pour l'oreille humaine, qu'aux ultrasons. L'expression « message sonique et/ou ultrasonique » désigne toute émission continue de signal

acoustique ininterrompu dans un intervalle de temps au début duquel le signal acoustique commence et à la fin duquel le signal acoustique s'arrête. Les termes « sonique » et « sonore » sont supposés être synonymes. Les termes « ultrasonique » et « ultrasonore » sont supposés être synonymes.

Le terme « codé » et ses dérivés appliqués à un message désignent le fait que ce message contient un code qui ne peut pas être décelé par un humain par la seule connaissance du message. Un message acoustique codé est donc inintelligible. Le terme « décoder » et ses dérivés, appliqués à un message codé, désignent le fait d'extraire le code transmis par le message codé. L'expression « cryptée » et ses dérivés désignent le fait qu'un signal, un ensemble de données, un message ou un code a fait l'objet d'un procédé de cryptage de telle sorte qu'il n'est compréhensible ni par l'homme ni par une machine ne possédant pas un procédé de décryptage permettant de récupérer le signal, l'ensemble de données, le message ou le code.

Préambule et art antérieur

On connaît déjà divers procédés d'authentification d'un utilisateur lors d'une transaction de type paiement par carte de crédit, par exemple durant un achat sur un site de e-commerce.

Parmi ces procédés, un des plus couramment utilisés à ce jour est le procédé dans lequel, une fois une transaction effectuée et le paiement requis en ligne par l'utilisateur sur un site de e-commerce, ledit utilisateur reçoit de la part de sa banque un code sous forme de SMS sur son téléphone mobile, et doit entrer ce code sur l'interface utilisateur de paiement de sa transaction pour authentifier celle-ci. Le fait que la personne effectuant la transaction dispose du téléphone mobile du titulaire du compte bancaire est considéré comme une preuve suffisante de l'identité de ce titulaire.

De même, lors d'un paiement dans un magasin par carte de crédit, il est courant que l'utilisateur vienne entrer son code secret sur un terminal de paiement pour valider sa transaction. Cette signature par entrée du code secret a cependant l'inconvénient du manque de sécurité engendré par la frappe du code devant d'autres personnes.

D'autres méthodes ont été envisagées pour pallier cet inconvénient, notamment par utilisation de e-carte de crédit, c'est-à-dire d'une carte de crédit

à usage unique, dont les données (dites OTP pour "One Time Password") sont générées à la demande de l'utilisateur pour un usage lors d'un unique achat.

On connaît encore la technologie des paiements par téléphones équipés pour le procédé de communication en champ proche (en anglais "Near Field Communication", d'où l'acronyme NFC). Dans cette technologie, un terminal émet à très courte distance (1 à 10 cm typiquement) un message haute fréquence électromagnétique vers un terminal récepteur pour transmettre une information de signature électronique.

Mais, à ce jour, seuls 3 à 5 % des téléphones mobiles sont compatibles avec la technologie NFC, ce qui limite l'utilisation d'authentification par ce moyen, et restreint, pour des raisons de coût, ses chances de généralisation auprès des commerçants ou clients.

US 2011/258121 (D1) décrit un procédé et un appareil pour permettre un paiement automatique dans lequel l'équipement de l'utilisateur souhaitant effectuer le paiement génère et émet un jeton audio, l'équipement du commerçant capte ce jeton audio, le décode et transmet une requête d'autorisation de paiement à un centre serveur distant. Le jeton audio généré par l'équipement utilisateur peut incorporer un mot de passe qui lui a été préalablement transmis par le centre serveur distant.

Ces différents procédés sont complexes ou manquent de sécurité pour l'utilisateur.

Exposé de l'invention

L'invention concerne donc un procédé d'authentification de transaction entre deux utilisateurs dudit procédé, un premier utilisateur étant doté d'un premier terminal mobile, un second utilisateur étant doté d'un second terminal mobile, au moins un de ces terminaux mobiles comportant des moyens d'émettre un signal en bande audio, et au moins l'autre terminal mobile comportant des moyens de recevoir un signal audio, ledit procédé comportant des étapes dans lesquelles :

- un mot de passe à usage unique est généré par un serveur d'authentification à la demande d'un des deux utilisateurs,

– ledit mot de passe à usage unique est transmis, via un réseau de communication, à destination d'un terminal mobile associé à un des utilisateurs,

– ledit mot de passe à usage unique est codé sous forme d'au moins un message sonique et/ou ultrasonique comportant au moins une partie du mot de passe à usage unique codée sous forme de sons et/ou d'ultrasons dans une bande de fréquences compatible avec une réception par un téléphone mobile,

– chaque message sonique et/ou ultrasonique est émis par un terminal mobile et écouté par l'autre terminal mobile,

– chaque message sonique et/ou ultrasonique reçu par un terminal mobile est retransmis par le terminal mobile à destination du serveur d'authentification pour comparaison avec un message attendu et pour validation,

caractérisé en ce que :

– le mot de passe à usage unique est coupé en au moins deux segments envoyés à l'un au moins des terminaux mobiles,

– les messages soniques et/ou ultrasoniques correspondant aux segments de mot de passe à usage unique sont échangés par voie sonique et/ou ultrasonique entre les terminaux mobiles,

– le serveur d'authentification reçoit les messages soniques et/ou ultrasoniques correspondant aux segments de mot de passe à usage unique de la part des terminaux mobiles, les décode pour en extraire les segments, et compare le message une fois reconstitué avec ledit mot de passe à usage unique pour validation.

Avantageusement et selon l'invention, le serveur d'authentification coupe le mot de passe à usage unique en au moins deux segments (en général plus de deux segments) et envoie ces segments à l'un au moins des terminaux mobiles. En variante ou en combinaison, dans certains modes de réalisation selon l'invention, au moins une partie du mot de passe à usage unique est coupée en au moins deux segments (en général plus de deux segments) par au moins l'un des terminaux (émetteur de messages soniques et/ou

ultrasoniques correspondant au moins à ces segments). Par ailleurs chaque segment peut ou non être crypté.

Par ailleurs, dans certains modes de réalisation selon l'invention, au moins une partie des segments du mot de passe à usage unique est codée en messages soniques et/ou ultrasoniques au niveau du serveur d'authentification avant transmission aux terminaux mobiles. En variante ou en combinaison, dans certains modes de réalisation selon l'invention, au moins une partie des segments du mot de passe à usage unique est codée en messages soniques et/ou ultrasoniques au niveau d'au moins un terminal mobile.

En outre dans certains modes de réalisation selon l'invention, les deux terminaux mobiles étant capables d'émettre et de recevoir des messages soniques et/ou ultrasoniques, le serveur d'authentification envoie au moins un segment (en général plusieurs segments) du mot de passe à usage unique à l'un des terminaux mobiles, et au moins un autre segment (en général plusieurs segments) du mot de passe à usage unique à l'autre des terminaux mobiles :

– les terminaux mobiles émettent des messages soniques et/ou ultrasoniques correspondant à chaque segment de mot de passe qu'ils ont reçu du serveur d'authentification,

– les terminaux mobiles écoutent lesdits messages soniques et/ou ultrasoniques et les transmettent au serveur d'authentification,

– le serveur d'authentification reçoit les messages soniques et/ou ultrasoniques de la part des terminaux mobiles, les décode pour en extraire les segments et reconstituer un message avec ces segments, et compare le message reconstitué avec ledit mot de passe à usage unique pour validation.

Dans certains modes de réalisation un procédé selon l'invention comporte une étape de vérification et validation des canaux de communication soniques et/ou ultrasoniques entre les deux terminaux mobiles avant d'envoyer les dits segments aux terminaux mobiles.

L'invention concerne ainsi en particulier un procédé d'authentification de transaction entre deux utilisateurs dudit procédé (dits client et commerçant), un premier utilisateur étant doté d'un premier terminal mobile, un second

utilisateur étant doté d'un second terminal mobile, au moins un de ces terminaux mobiles comportant des moyens d'émettre un signal en bande audio, et au moins l'autre terminal mobile comportant des moyens de recevoir un signal en bande audio. On utilise donc des ondes acoustiques pour échanger des informations entre les deux dispositifs de manière sécurisée.

Le procédé comporte des étapes dans lesquelles :

- un message d'authentification est généré par un serveur d'authentification à la demande d'un des deux utilisateurs,

- ledit message d'authentification est transmis, via un réseau de communication, à destination d'un terminal mobile associé à un des utilisateurs,

- ledit message d'authentification est codé sous forme de message sonique et/ou ultrasonique comportant au moins une partie du message codée sous forme de sons ou d'ultrasons dans la bande de fréquences compatible avec une réception par un téléphone mobile classique,

- ledit message sonique et/ou ultrasonique est émis par ledit terminal mobile et écouté par l'autre terminal mobile, associé à l'autre utilisateur,

- le message sonique et/ou ultrasonique reçu est retransmis par le second terminal mobile à destination du serveur d'authentification pour comparaison avec le message attendu et pour validation.

Le processus d'authentification comprend deux facteurs de sécurité : le premier est le nom de l'utilisateur et le code PIN, qui garantit l'identité de l'utilisateur, et le second consiste dans un code sonique et/ou ultrasonique qui garantit la proximité et la possession des dispositifs qui interviennent dans la transaction. Il s'agit d'une authentification en champ proche.

Dans une mise en œuvre particulière, la transformation du message d'authentification en message sonique et/ou ultrasonique est réalisée au niveau du serveur d'authentification avant transmission au terminal mobile,

Dans une mise en œuvre plus particulière, le serveur d'authentification est alors par exemple de type IVR ("Interactive Voice Response server").

Dans une mise en œuvre alternative, la transformation (codage et éventuellement brouillage) du message d'authentification en message sonique et/ou ultrasonique est réalisée au niveau du terminal mobile.

Dans une mise en œuvre particulière, le message d'authentification est de type à usage unique (OTP), spécifique à chaque transaction à signer. Cette disposition garantit une sécurité accrue de la transaction.

Dans une mise en œuvre particulière, le procédé comporte une étape de vérification et de validation des canaux de communication soniques et/ou ultrasoniques entre les deux terminaux mobiles. De cette manière, le procédé s'adapte aux conditions existantes au niveau du commerçant et du client, et optimise la force de l'authentification en fonction de ces canaux de communication disponibles. Il est notamment capable d'utiliser éventuellement les capacités ultrasonores des terminaux, si ceux-ci en sont dotés.

Dans une première mise en œuvre, un premier terminal mobile, dit "terminal de paiement du commerçant" étant supposé doté de moyens d'écouter un message sonique et/ou ultrasonique et de le retransmettre à destination d'un serveur dit "serveur d'authentification", et un second terminal mobile, de type téléphone mobile, dit "téléphone mobile du client", étant supposé doté d'une application logicielle adaptée à transformer (codage et éventuellement brouillage) un message reçu du serveur d'authentification, le procédé comporte notamment des étapes suivantes :

- étape 301 : le terminal de paiement du commerçant émet une demande d'autorisation de transaction à destination du serveur d'authentification,

- étape 302 : le serveur d'authentification, vérifie les moyens de communication soniques et/ou ultrasoniques existant entre le terminal de paiement du commerçant et le téléphone mobile du client,

- étape 303 : dans le cas où les deux terminaux sont capables d'émettre et de recevoir des messages soniques et/ou ultrasoniques, le serveur d'authentification obtient ou génère un mot de passe à usage unique, puis coupe alors ce mot de passe en au moins deux segments (en général plus de deux segments), et envoie au moins un segment (notamment certains de ces segments) au terminal de paiement, et au moins un autre segment (notamment les autres segments) au téléphone mobile du client, au moins une partie de ces segments du mot de passe à usage unique étant transformée (codée et éventuellement brouillée et/ou cryptée) par le terminal de paiement ou le téléphone mobile en messages soniques et/ou ultrasoniques dans une bande

de fréquence compatible avec les moyens d'émission dudit terminal de paiement et avec les moyens de réception d'un téléphone mobile,

- le terminal de paiement et le téléphone mobile émettent les messages soniques et/ou ultrasoniques correspondant aux segments de mot de passe qu'ils ont reçu du serveur d'authentification,

- étape 304 : le téléphone mobile du client et le terminal de paiement écoutent lesdits messages soniques et/ou ultrasoniques et les enregistrent, puis transmettent ces enregistrements au serveur d'authentification,

- étape 305 : le serveur d'authentification reçoit les enregistrements des messages soniques et/ou ultrasoniques de la part du téléphone mobile du client et du terminal de paiement, décode ces messages soniques et/ou ultrasoniques pour en extraire les segments, et compare ce message reconstitué avec le mot de passe original pour validation.

Dans une autre mise en œuvre, le second terminal mobile, de type téléphone mobile, dit "téléphone mobile du client", étant supposé doté d'une application logicielle adaptée à transformer un message reçu d'un serveur associé au générateur d'authentification, dit "serveur d'authentification", en message sonique et/ou ultrasonique ayant éventuellement subi une distorsion volontaire (brouillage), le premier terminal mobile, dit "terminal de paiement du commerçant" étant doté de moyens d'écouter un message sonique et/ou ultrasonique et de le retransmettre à destination du serveur d'authentification et doté de moyens de générer un mot de passe à usage unique, le procédé comporte notamment des étapes suivantes :

- étape 401 : le terminal de paiement du commerçant émet une demande d'autorisation de transaction à destination du serveur d'authentification et initialise la transaction,

- étape 402 : le terminal de paiement vérifie les moyens de communication soniques et/ou ultrasoniques existant entre le terminal de paiement du commerçant et le téléphone mobile du client,

- étape 403 : dans le cas favorable, le terminal de paiement coupe le mot de passe généré par le serveur d'authentification en au moins deux segments, envoie au moins un segment (notamment certains de ces segments) au téléphone mobile du client par l'intermédiaire du serveur d'authentification, et

au moins un autre segment (notamment les autres segments) par voie sonique et/ou ultrasonique,

- étape 404 : le téléphone mobile du client écoute le message sonique et/ou ultrasonique reçu du terminal de paiement et l'enregistre, puis transmet cet enregistrement au terminal de paiement via ledit serveur d'authentification,

- étape 405 : le terminal de paiement reçoit les informations de la part du téléphone mobile du client, en extrait le message original, et compare ce message une fois reconstitué avec le mot de passe original.

Plus particulièrement dans ce cas, dans l'étape 404, la transmission de l'enregistrement et du segment de message reçu est effectuée par l'intermédiaire du serveur d'authentification.

Alternativement, dans l'étape 404, une partie au moins de l'enregistrement et de chaque segment de message reçu est émise sous forme sonique et/ou ultrasonique par le téléphone mobile du client vers le terminal de paiement.

Dans une variante, le message d'authentification à usage unique fourni par le serveur d'authentification est codé par le serveur d'authentification lui-même sous forme de message sonique et/ou ultrasonique, le serveur d'authentification, étant en relation avec un server de type VoIP (voix sur IP), c'est-à-dire capable de générer des appels téléphoniques et des signaux dans une bande de fréquences soniques et/ou ultrasoniques.

L'invention vise sous un second aspect un terminal de paiement, un téléphone mobile ou un serveur d'authentification, mettant en œuvre un procédé selon l'invention.

Présentation des figures

Les caractéristiques et avantages de l'invention seront mieux appréciés grâce à la description qui suit, description qui expose les caractéristiques de l'invention au travers d'un exemple non limitatif d'application.

La description s'appuie sur les figures annexées qui représentent :

Figure 1 : un schéma des éléments mis en œuvre dans le procédé,

Figure 2 : un schéma des étapes du procédé dans un premier mode de mise en œuvre,

Figure 3 : un schéma des étapes de procédé dans une variante de ce premier mode de mise en œuvre,

Figure 4 : un schéma des étapes de procédé dans un second mode de mise en œuvre,

Figure 5 : un schéma des étapes de procédé dans un troisième mode de mise en œuvre.

Description détaillée d'un mode de réalisation de l'invention

Comme on le voit sur la figure 1, l'invention trouve sa place dans le cadre d'une transaction entre un premier utilisateur 10 appelé commerçant dans la suite de la description, et un second utilisateur 11 appelé client dans la suite de la description.

Le commerçant 10 est supposé dote d'un terminal de paiement 12 comportant des moyens de communication, via un réseau 14, par exemple de type GSM, avec un serveur d'authentification 13 capable de fournir des autorisations de transactions. Dans le présent exemple de réalisation, le terminal de paiement 12 du commerçant 10 est également supposé doté d'un haut-parleur adapté à émettre un message sonique et/ou ultrasonique en bande compatible avec la bande de fréquences d'émission et/ou de réception d'un téléphone mobile.

Le client 11 est supposé doté d'un terminal mobile 15 de type téléphone mobile ou tablette ou TPE ou caisse enregistreuse, doté de moyens de communication via un réseau de communications 14, par exemple GSM, avec divers services à distance. Ce téléphone mobile 15 comporte naturellement un microphone capable de recevoir un signal audio et un haut-parleur pour émettre un signal audio, dans une bande de fréquences comportant la bande de fréquence audible par l'oreille humaine et éventuellement la bande ultrasonique.

L'invention est destinée à être mise en œuvre sous forme logicielle. Dans certains modes de réalisation au moins un logiciel est installé dans le serveur d'authentification 13, et au moins un logiciel est installé dans le terminal de paiement 12 du commerçant 10.

Dans certains modes de réalisation, au moins un logiciel est également installé dans le téléphone mobile 15 du client 11, sous forme par exemple d'application smartphone (ordiphone) de type "apps".

Mode de fonctionnement

Dans un premier mode de mise en œuvre, illustré par la figure 2, le procédé d'authentification de transaction comporte cinq étapes principales, pour valider un paiement réalisé par le client 11 chez le commerçant 10.

Dans cette mise en œuvre, le téléphone mobile 15 du client 11 est supposé doté d'une application logicielle adaptée à transformer (coder et éventuellement brouiller) tout ou partie de l'OTP émis par le serveur d'authentification 13, en message sonique et/ou ultrasonique. Le serveur d'authentification 13 est celui qui génère le mot de passe à usage unique (OTP).

De même, dans cette première mise en œuvre, le terminal de paiement 12 est supposé doté de moyens d'écouter un message sonique et/ou ultrasonique et de le retransmettre à destination du serveur d'authentification 13.

Dans une première étape 301, le terminal de paiement 12 du commerçant 10 émet une demande d'autorisation de transaction à destination du serveur d'authentification 13.

Dans une seconde étape 302, le serveur d'authentification 13 vérifie et valide les canaux de communication soniques et/ou ultrasoniques entre les deux terminaux mobiles 12, 15 avant d'envoyer les dits segments aux terminaux mobiles. Le serveur d'authentification 13 vérifie les moyens de communication existants entre le terminal de paiement 12 du commerçant 10 et le téléphone mobile 15 du client 11. Cette étape consiste à vérifier lesquels des deux terminaux 12, 15 sont capables d'émettre et/ou de recevoir des messages soniques et/ou ultrasoniques.

À cet effet, dans le présent exemple nullement limitatif, le serveur d'authentification, ici associé à un serveur de type VoIP, émet des sons et/ou ultrasons via le réseau de communication TCP/IP à destination du terminal de paiement 12 du commerçant et via le réseau de téléphonie mobile, ici GSM, à destination du téléphone mobile 15 du client 11, afin de reconnaître les voies

de communication audio disponibles entre le terminal de paiement 12 et le téléphone mobile 15. Les messages acoustiques soniques et/ou ultrasoniques reçus par le haut-parleur du terminal de paiement sont retransmis au serveur d'authentification via le même réseau. Il en va de même des messages acoustiques soniques et/ou ultrasoniques reçus par le haut-parleur du terminal mobile. Le serveur analyse ces messages et détermine de la sorte les voies de communication audio possibles entre le terminal de paiement 12 et le téléphone mobile 15, c'est-à-dire concrètement entre le haut-parleur du terminal de paiement 12 et le microphone du téléphone mobile 15, et/ou entre le haut-parleur du téléphone mobile 15 et le microphone du terminal de paiement 12.

Lors de la détermination des voies de communication possibles, le serveur d'authentification 13 teste également la capacité de chacun des terminaux mobiles en émission et en réception de message dans le domaine sonore et/ou ultrasonore. De la sorte, le système peut utiliser au mieux les capacités de chaque groupe de deux terminaux, et notamment s'adapter aux téléphones mobiles plus anciens, qui ne possèdent pas de capacité ultrasonore.

Le test peut être réalisé lors de chaque transaction, le procédé permet de s'adapter également à des variations dans le temps des capacités des terminaux mobiles, ou à des conditions d'environnement sonore difficiles (bruits extérieurs etc.). Dans ces cas, le codage du message est avantageusement réalisé dans les fréquences les mieux reçues par les terminaux mobiles et / ou les moins bruitées.

Dans le cas où le terminal de paiement 12 n'est pas capable d'écouter des signaux acoustiques, le procédé est détaillé plus bas (étapes 303' à 306').

Dans le cas où les deux terminaux 12, 15 sont capables d'émettre et de recevoir des messages soniques et/ou ultrasoniques, dans une étape 303, le serveur d'authentification 13 génère un mot de passe à usage unique. Alternativement, le serveur d'authentification 13 ne génère pas lui-même ce mot de passe à usage unique, mais le reçoit d'un service de gestion de mots de passe, éventuellement distant. Ce service de gestion de mots de passe est

alors adapté à générer un mot de passe à usage unique, et à authentifier un tel mot de passe lorsqu'il est reçu.

Le serveur d'authentification 13 coupe alors ce mot de passe en segments de façon aléatoire, et envoie certains de ces segments au terminal de paiement 12, et les autres segments au téléphone mobile 15 du client. Dans le présent exemple de mise en œuvre, le mot de passe est coupé en deux segments de longueurs éventuellement différentes. Dans une variante, il est scindé en multiples segments.

Toujours dans cette étape 303, chacun de ces segments du mot de passe à usage unique est transformé par le terminal de paiement 12 et le téléphone mobile 15 en messages soniques et/ou ultrasoniques dans la bande de fréquence compatible avec les moyens d'émission dudit terminal de paiement 12 et avec les moyens de réception d'un téléphone mobile. Le terminal de paiement 12 et le téléphone mobile 15 émettent les messages soniques et/ou ultrasoniques correspondant aux segments de mot de passe qu'ils ont reçu du serveur d'authentification 13.

Dans une étape 304, le téléphone mobile 15 du client 11, et le terminal de paiement 12 écoutent lesdits messages soniques et/ou ultrasoniques et les enregistrent, puis transmettent ces enregistrements au serveur d'authentification 13.

Enfin, dans une étape 305, le serveur d'authentification 13 reçoit les enregistrements des messages soniques et/ou ultrasoniques de la part du téléphone mobile 15 du client 12 et du terminal de paiement 12 du commerçant 10.

Le serveur d'authentification 13 transforme ces messages soniques et/ou ultrasoniques de façon inverse pour en extraire les segments du message original, et compare ce message une fois reconstitué avec le mot de passe original.

Le serveur d'authentification 13 notifie alors au client 11 via son téléphone mobile 15 et au commerçant 10 via son terminal de paiement 12 la réussite ou l'échec de la signature de la transaction.

Dans une variante de cette mise en œuvre, dans le cas où le terminal de paiement est capable de recevoir des messages soniques et/ou ultrasoniques,

et où le téléphone mobile est doté d'une application logicielle spécifique, l'ensemble du mot de passe est envoyé au téléphone mobile 15 du client 11. Il est alors émis sous forme sonique et/ou ultrasonique et reçu par le terminal de paiement 12, qui le renvoie vers le serveur d'authentification 13 via le réseau TCP/IP pour validation. Il s'agit alors d'un mode de mise en œuvre similaire à la première mise en œuvre du procédé, telle que décrite plus haut, en renversant les rôles du terminal de paiement 12 et du téléphone mobile 15.

Après l'étape 302 de détermination par le serveur d'authentification, des voies de communication audio possibles entre le terminal de paiement 12 et le téléphone mobile 15, lorsque le terminal de paiement est capable seulement d'émettre des messages soniques et/ou ultrasoniques, mais pas de les recevoir, le procédé comporte, dans un exemple non limitatif de mise en œuvre, des étapes suivantes (voir figure 3).

Dans une étape 303', le serveur d'authentification 13 génère un tel mot de passe à usage unique. Alternativement, le serveur d'authentification 13 ne génère pas lui-même ce mot de passe à usage unique, mais le reçoit d'un service de gestion de mots de passe, éventuellement distant. Ce service de gestion de mots de passe est alors adapté à générer un mot de passe à usage unique, et à authentifier un tel mot de passe lorsqu'il est reçu.

Le mot de passe à usage unique, usuellement une suite de caractères ou de chiffres, est envoyé au terminal de paiement 12 du commerçant 10, et transformé par ledit terminal de paiement en message sonique et/ou ultrasonique dans la bande de fréquence compatible avec les moyens d'émission dudit terminal de paiement 12 et avec les moyens de réception d'un téléphone mobile. Il s'agit ici d'un message comportant au moins une partie codée sous forme de sons ou/et d'ultrasons, non audibles ou audibles par l'homme mais entrant dans la bande de fréquences reçue correctement par un téléphone mobile. Simultanément, le serveur d'authentification, appelle le téléphone mobile 15 du client 11, qui décroche, de manière à être prêt à recevoir le message sonique.

Dans une étape 304', le terminal de paiement 12 émet le message sonique par l'intermédiaire de son haut-parleur.

Dans une étape 305', le téléphone mobile 15 du client 11 écoute ledit message sonique par son microphone, et l'enregistre, puis le transmet au serveur d'authentification 13.

Enfin, dans une étape 306', le serveur d'authentification 13 reçoit l'enregistrement du message sonique de la part du téléphone mobile 15 du client 12, le transforme de façon inverse pour en extraire le message original, et compare ce message avec le message émis à destination du terminal de paiement 12 chez le commerçant 11. Le serveur d'authentification 13 notifie alors au client 11 via son téléphone mobile 15 et au commerçant 10 via son terminal de paiement 12 la réussite ou l'échec de la signature de la transaction.

Dans un second mode de mise en œuvre, illustré par la figure 4, le procédé d'authentification de transaction comporte encore cinq étapes principales, pour valider un paiement réalisé par le client 11 chez le commerçant 10.

Dans cette seconde mise en œuvre, le téléphone mobile 15 du client 11 est encore supposé doté d'une application logicielle adaptée à transformer ou brouiller un OTP reçu du serveur d'authentification 13 en message sonique et/ou ultrasonique.

De même, dans cette seconde mise en œuvre, le terminal de paiement 12 est encore supposé doté de moyens d'écouter un message sonique et/ou ultrasonique et de le retransmettre à destination du serveur d'authentification 13. Il est également supposé ici doté de moyens de transformer (coder et éventuellement brouiller) un mot de passe à usage unique.

Dans une première étape 401, le terminal de paiement 12 du commerçant 10 émet une demande d'autorisation de transaction à destination du serveur d'authentification 13 et initialise la transaction.

Dans une seconde étape 402, le terminal de paiement 12 vérifie et valide les moyens de communication existant entre le terminal de paiement 12 du commerçant 10 et le téléphone mobile 15 du client 11. Cette étape consiste à vérifier si les deux terminaux 12, 15 sont capables d'émettre et de recevoir des messages soniques et/ou ultrasoniques, et de préciser dans quelles bandes de fréquences acoustiques ils sont capables de communiquer en émission et réception, et éventuellement quelles sont les bandes les plus efficaces.

Dans le cas favorable, dans une étape 403, le terminal de paiement 12 génère un mot de passe à usage unique. Le terminal de paiement 12 coupe alors ce mot de passe en segments de façon aléatoire, et envoie au téléphone mobile 15 du client 11 certains de ces segments par l'intermédiaire du serveur d'authentification 13, et les autres segments par voie sonique et/ou ultrasonique au client 11. Dans le présent exemple de mise en œuvre, le mot de passe est coupé en deux segments de longueurs éventuellement différentes. Dans une variante, il est scindé en multiples segments.

Dans une étape 404, le téléphone mobile 15 du client 11 écoute le message sonique et/ou ultrasonique reçu du terminal de paiement et l'enregistre, puis transmet cet enregistrement et le segment de message reçu par l'intermédiaire du serveur d'authentification 13 au terminal de paiement 12 via ledit serveur d'authentification 13.

Alternativement, une partie ou la totalité de ces informations est émise sous forme sonique et/ou ultrasonique par le téléphone mobile 15 du client 11 vers le terminal de paiement 12.

Enfin, dans une étape 405, le terminal de paiement 12 reçoit les informations de la part du téléphone mobile 15 du client 11, en extrait le message original, et compare ce message une fois reconstitué avec le mot de passe original.

Le terminal de paiement 12 notifie alors au téléphone mobile 15 du client 11 via le serveur d'authentification 13 la réussite ou l'échec de la signature de la transaction.

Dans un troisième mode de mise en œuvre, illustré par la figure 5, le procédé d'authentification de transaction concerne un cas où ni le téléphone mobile 15 du client 11, ni le terminal de paiement 12 ne sont dotés d'applications spécifiques pour mettre en œuvre le procédé. De cette manière, le procédé est utilisable très facilement, y compris par des personnes désirant effectuer une transaction et non équipées d'applications spécifiques.

Le serveur d'authentification 13 est, quant à lui, associé à un serveur de type serveur IVR ("Interactive Voice Response"), apte à générer et recevoir des messages sonores.

De même, dans cette troisième mise en œuvre, le terminal de paiement 12 est encore supposé doté de moyens d'écouter un message sonique et de le retransmettre à destination du serveur d'authentification 13. Il peut s'agir d'un téléphone mobile.

Dans une première étape 501, le terminal de paiement 12 du commerçant 10 appelle le serveur d'authentification 13.

Dans une étape 502, il émet une demande d'autorisation de transaction en envoyant son identifiant de terminal de paiement, le numéro de téléphone du client et le montant de la transaction qui doit être réalisée.

Dans une étape 503, le serveur d'authentification 13 vérifie les données reçues, et appelle le numéro du téléphone mobile du client. Le serveur d'authentification 13 génère un mot de passe à usage unique le scinde en segments, et code ces segments en messages soniques.

Dans une étape 504, le client entre un code de validation (de type code pin de carte de crédit) sur son téléphone mobile 15 qui envoie ces données au serveur d'authentification 13.

Dans une étape 505, le terminal de paiement 12 et le téléphone mobile 15 sont rapprochés et le mot de masse codé sous forme de messages soniques par le serveur d'authentification de type IVR est transmis à ces terminaux, qui échangent ces messages soniques entre eux par voix sonique. Le serveur d'authentification 13 reçoit ensuite chaque message sonique tel que reçu par voie audio par chaque terminal et retransmis au serveur d'authentification 13.

Le serveur d'authentification 13 notifie alors dans une étape 506 au client 11 via son téléphone mobile 15 et au terminal de paiement 12 la réussite ou l'échec de la signature de la transaction.

Dans une variante de cette troisième mise en œuvre, le serveur vérifie et valide les moyens de communication, de façon analogue à ce qui a été décrit pour la première mise en œuvre,

Dans une autre variante, le serveur scinde le mot de passe sonique en multiples segments et les envoie sur les différentes voies de communication validées, de façon analogue à ce qui a été décrit pour la seconde mise en œuvre du procédé.

Dans toute la description qui précède, il a été fait référence à une transaction de type paiement d'un achat. Il est clair que le procédé selon l'invention s'applique plus largement à tout type d'authentification en champ proche, permettant à deux terminaux de communiquer de façon sécurisée.

L'invention peut faire l'objet de nombreuses variantes et modes de réalisation par rapport aux seuls modes de réalisation décrits ci-dessus et représentés sur les dessins. En particulier, l'invention peut être appliquée avec un très grand nombre de catégories différentes de terminaux. En particulier, avantageusement et selon l'invention chaque terminal mobile est choisi dans le groupe formé des téléphones mobiles (cellulaires portatifs ou par satellite portatifs), des ordiphones (téléphones cellulaires informatiques portatifs, dits « smartphones » en anglais), des tablettes tactiles informatiques portatives, des ordinateurs portables, des terminaux de paiement électronique (TPE). Il est à noter en particulier que l'invention permet de sécuriser et d'authentifier une communication entre des terminaux mobiles extrêmement simples, en particulier lorsque l'un au moins d'entre eux est un simple téléphone mobile cellulaire portatif de type GSM (et non un ordiphone (téléphone mobile (portatif cellulaire) informatique, (doté de moyens de traitement de données numériques)), ou lorsque tous les terminaux sont de simples téléphones mobiles cellulaires portatifs de type GSM. L'invention permet donc de sécuriser et d'authentifier des communications dans les régions du monde non (ou peu) équipées d'ordiphones et de réseaux (UMTS, LTE, 3G, 4G…) permettant l'exploitation de ces ordiphones.

REVENDICATIONS

1/ - Procédé d'authentification de transaction entre deux utilisateurs dudit procédé, un premier utilisateur étant doté d'un premier terminal mobile, un second utilisateur étant doté d'un second terminal mobile, au moins un de ces terminaux mobiles (12, 15) comportant des moyens d'émettre un signal en bande audio, et au moins l'autre terminal mobile comportant des moyens de recevoir un signal audio, ledit procédé comportant des étapes dans lesquelles :

- un mot de passe à usage unique est généré par un serveur d'authentification (13) à la demande d'un des deux utilisateurs,
- ledit mot de passe à usage unique est transmis, via un réseau de communication, à destination d'un terminal mobile associé à un des utilisateurs,
- ledit mot de passe à usage unique est codé sous forme d'au moins un message sonique et/ou ultrasonique comportant au moins une partie du mot de passe à usage unique codée sous forme de sons et/ou d'ultrasons dans une bande de fréquences compatible avec une réception par un téléphone mobile,
- chaque message sonique et/ou ultrasonique est émis par un terminal mobile et écouté par l'autre terminal mobile,
- chaque message sonique et/ou ultrasonique reçu par un terminal mobile est retransmis par le terminal mobile à destination du serveur d'authentification (13) pour comparaison avec un message attendu et pour validation,

caractérisé en ce que :

- le mot de passe à usage unique est coupé en au moins deux segments envoyés à l'un (12) au moins des terminaux mobiles,
- les messages soniques et/ou ultrasoniques correspondant aux segments de mot de passe à usage unique sont échangés par voie sonique et/ou ultrasonique entre les terminaux mobiles (12, 15),
- le serveur d'authentification (13) reçoit les messages soniques et/ou ultrasoniques correspondant aux segments de mot de passe à usage unique de la part des terminaux mobiles, les décode pour en extraire les

segments, et compare le message une fois reconstitué avec ledit mot de passe à usage unique pour validation.

2/ - Procédé selon la revendication 1, caractérisé en ce que le serveur d'authentification (13) coupe le mot de passe à usage unique en au moins deux segments et envoie ces segments à l'un (12) au moins des terminaux mobiles.

3/ - Procédé selon l'une des revendications 1 ou 2, caractérisé en ce qu'au moins une partie des segments du mot de passe à usage unique est codée en messages soniques et/ou ultrasoniques au niveau du serveur d'authentification (13) avant transmission aux terminaux mobiles.

4/ - Procédé selon l'une des revendications 1 à 3, caractérisé en ce qu'au moins une partie des segments du mot de passe à usage unique est codée en messages soniques et/ou ultrasoniques au niveau d'au moins un terminal mobile.

5/ - Procédé selon l'une des revendications 1 à 4, caractérisé en ce que les deux terminaux mobiles (12, 15) étant capables d'émettre et de recevoir des messages soniques et/ou ultrasoniques, le serveur d'authentification (13) envoie au moins un segment du mot de passe à usage unique à l'un (12) des terminaux mobiles, et au moins un autre segment du mot de passe à usage unique à l'autre (15) des terminaux mobiles,

– les terminaux mobiles (12, 15) émettent des messages soniques et/ou ultrasoniques correspondant à chaque segment de mot de passe qu'ils ont reçu du serveur d'authentification (13),

– les terminaux mobiles (12, 15) écoutent lesdits messages soniques et/ou ultrasoniques et les transmettent au serveur d'authentification (13),

– le serveur d'authentification (13) reçoit les messages soniques et/ou ultrasoniques de la part des terminaux mobiles, les décode pour en extraire les segments et reconstituer un message avec ces segments, et compare le message reconstitué avec ledit mot de passe à usage unique pour validation.

6/ - Procédé selon la revendication 5, caractérisé en ce qu'il comporte une étape de vérification et validation des canaux de

communication soniques et/ou ultrasoniques entre les deux terminaux mobiles (12, 15) avant d'envoyer les dits segments aux terminaux mobiles.

7/ - Procédé selon l'une quelconque des revendications 1 à 6, le second terminal mobile (15), de type téléphone mobile, dit "téléphone mobile du client", étant supposé doté d'une application logicielle adaptée à transformer un message reçu d'un serveur dit serveur d'authentification (13) en message sonique, et le premier terminal mobile (12), dit "terminal de paiement du commerçant" étant supposé doté de moyens d'écouter un message sonique et/ou ultrasonique et de le retransmettre à destination du serveur d'authentification (13),

caractérisé en ce qu'il comporte notamment des étapes suivantes :

– étape 301 : le terminal de paiement (12) émet une demande d'autorisation de transaction à destination du serveur d'authentification (13),

– étape 302 : le serveur d'authentification (13) vérifie les moyens de communication soniques et/ou ultrasoniques existant entre le terminal de paiement (12) et le téléphone mobile (15) du client (11),

– étape 303 : dans le cas où les deux terminaux mobiles (12, 15) sont capables d'émettre et de recevoir des messages soniques et/ou ultrasoniques, le serveur d'authentification (13) obtient un mot de passe à usage unique, puis coupe alors ce mot de passe en au moins deux segments, et envoie au moins un segment au terminal de paiement (12), et au moins un autre segment au téléphone mobile (15) du client,

– le terminal de paiement (12) et le téléphone mobile (15) émettent des messages soniques et/ou ultrasoniques correspondant à chaque segment de mot de passe qu'ils ont reçu du serveur d'authentification (13),

– étape 304 : le téléphone mobile (15) du client et le terminal de paiement (12) écoutent lesdits messages soniques et/ou ultrasoniques et les enregistrent, puis transmettent ces enregistrements au serveur d'authentification (13),

– étape 305 : le serveur d'authentification (13) reçoit les enregistrements des messages soniques et/ou ultrasoniques de la part du

téléphone mobile (15) du client et du terminal de paiement (12), décode ces messages soniques et/ou ultrasoniques pour en extraire les segments et reconstituer un message avec ces segments, et compare ce message reconstitué avec le mot de passe original pour validation.

8/ - Procédé selon l'une quelconque des revendications 1 à 6, le second terminal mobile, de type téléphone mobile, dit "téléphone mobile du client", étant doté d'une application logicielle adaptée à transformer un message reçu d'un serveur d'authentification (13) associé au générateur d'authentification, dit "serveur d'authentification ", en message sonique et/ou ultrasonique, le premier terminal mobile (12), dit "terminal de paiement du commerçant" étant doté de moyens d'écouter un message sonique et/ou ultrasonique et de le retransmettre à destination du serveur d'authentification (13), ledit serveur d'authentification étant doté de moyens de générer un mot de passe à usage unique,

caractérisé en ce qu'il comporte notamment des étapes suivantes :

– étape 401 : un premier terminal mobile, dit "terminal de paiement" (12) émet une demande d'autorisation de transaction à destination du serveur d'authentification (13) et initialise la transaction,

– étape 402 : le terminal de paiement (12) vérifie les moyens de communication soniques et/ou ultrasoniques existants entre le terminal de paiement (12) du commerçant et le téléphone mobile (15) du client,

– étape 403 : dans le cas favorable, le terminal de paiement (12) coupe le mot de passe à usage unique généré par le serveur d'authentification (13) en au moins deux segments, envoie au moins un segment au téléphone mobile (15) du client par l'intermédiaire du serveur d'authentification (13), et au moins un autre segment par voie sonique et/ou ultrasonique,

– étape 404 : le téléphone mobile (15) du client écoute le message sonique et/ou ultrasonique reçu du terminal de paiement et l'enregistre, puis transmet cet enregistrement au terminal de paiement (12) via ledit serveur d'authentification (13),

– étape 405 : le terminal de paiement (12) reçoit les informations de la part du téléphone mobile (15) du client, en extrait chaque

segment, et compare le message une fois reconstitué avec le mot de passe à usage unique.

9/ - Procédé selon la revendication 8, caractérisé en ce que, dans l'étape 404, une partie au moins de l'enregistrement et de chaque segment reçu du serveur d'authentification (13) est émise sous forme sonique et/ou ultrasonique par le téléphone mobile (15) du client vers le terminal de paiement (12)

10/ - Procédé selon l'une quelconque des revendications 1 à 9, caractérisé en ce qu'il comporte des étapes dans lesquelles :

- un message d'authentification est généré par un serveur d'authentification (13) à la demande d'un des deux utilisateurs,

- ledit message d'authentification est transmis, via un réseau de communication, à destination d'un terminal mobile associé à un des utilisateurs,

- ledit message d'authentification est codé sous forme de message sonique et/ou ultrasonique comportant au moins une partie du message codée sous forme de sons et/ou d'ultrasons dans la bande de fréquences compatible avec une réception par un téléphone mobile classique,

- ledit message sonique est émis par ledit terminal mobile et écouté par l'autre terminal mobile, associé à l'autre utilisateur,

- le message sonique et/ou ultrasonique reçu est retransmis par le second terminal mobile à destination du serveur d'authentification (13) pour comparaison avec le message attendu et pour validation.

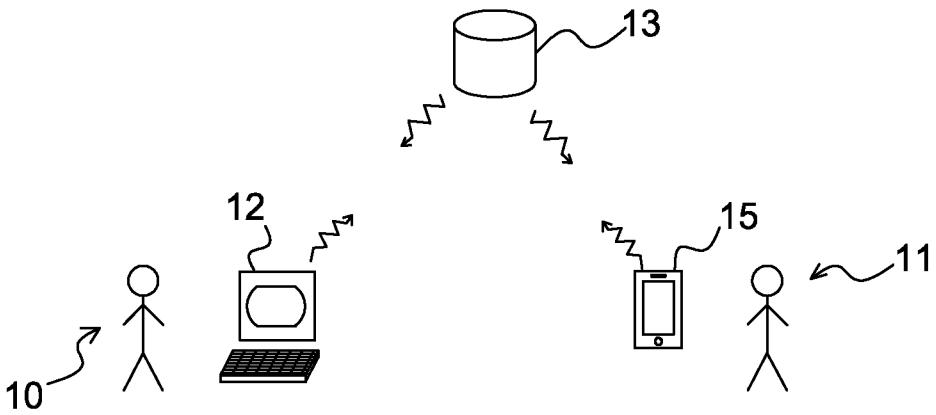
13
12
15
11
10

Fig.1

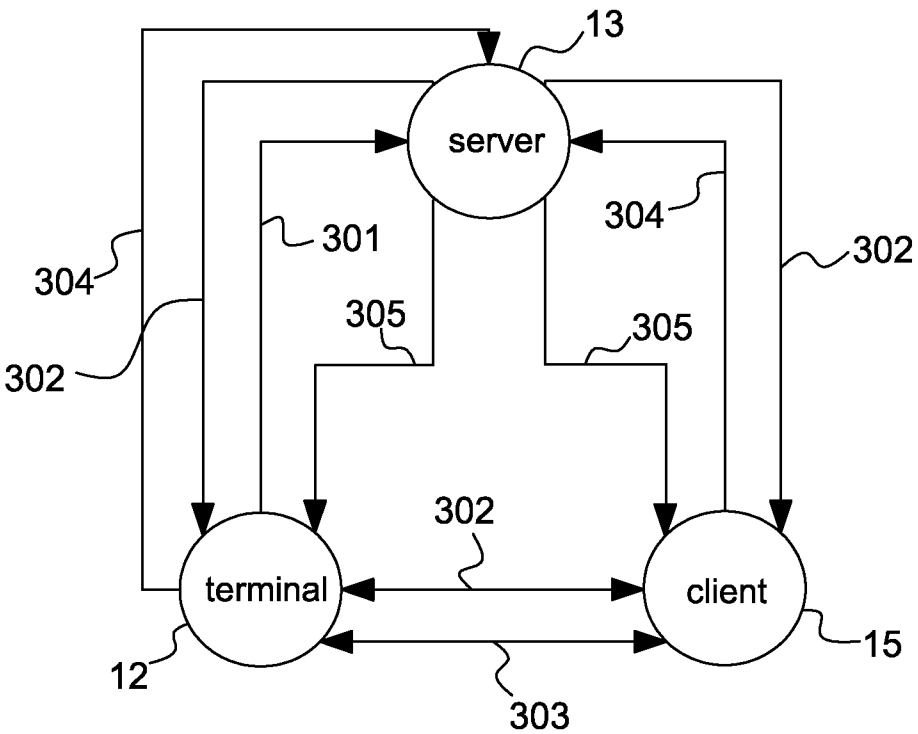
13
server
304
301
304
302
305
305
302
302
terminal
client
12
15
303

Fig.2

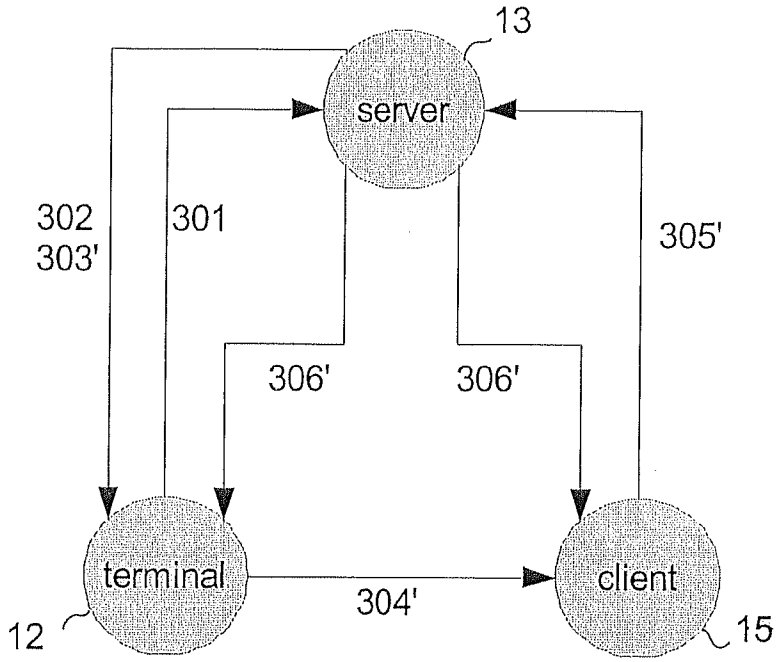
13
server
302
303'
301
305'
306'
306'
terminal
304'
client
12
15

Fig. 3

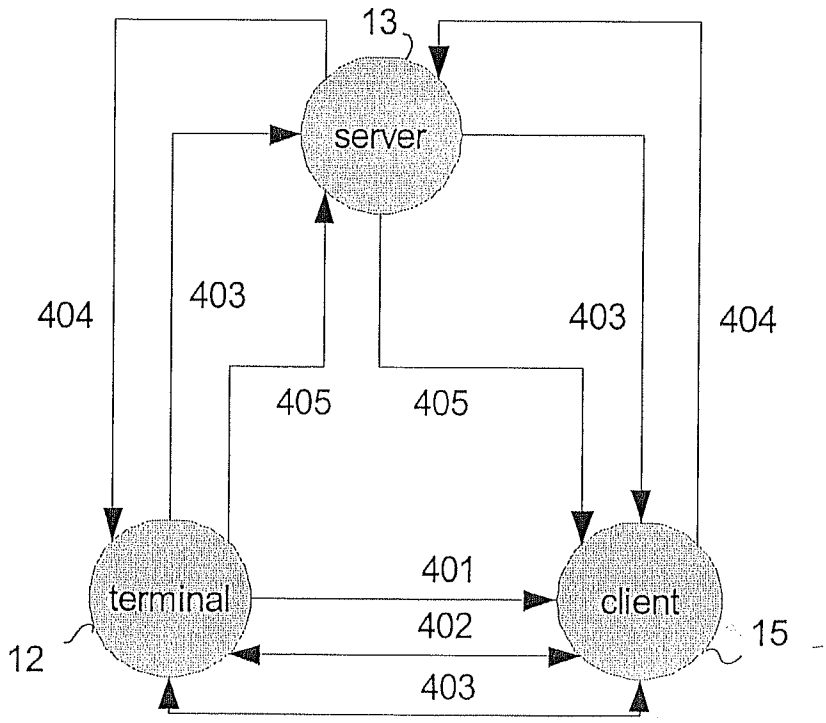
13
server
404
403
403
404
405
405
401
terminal
client
402
12
15
403

Fig. 4

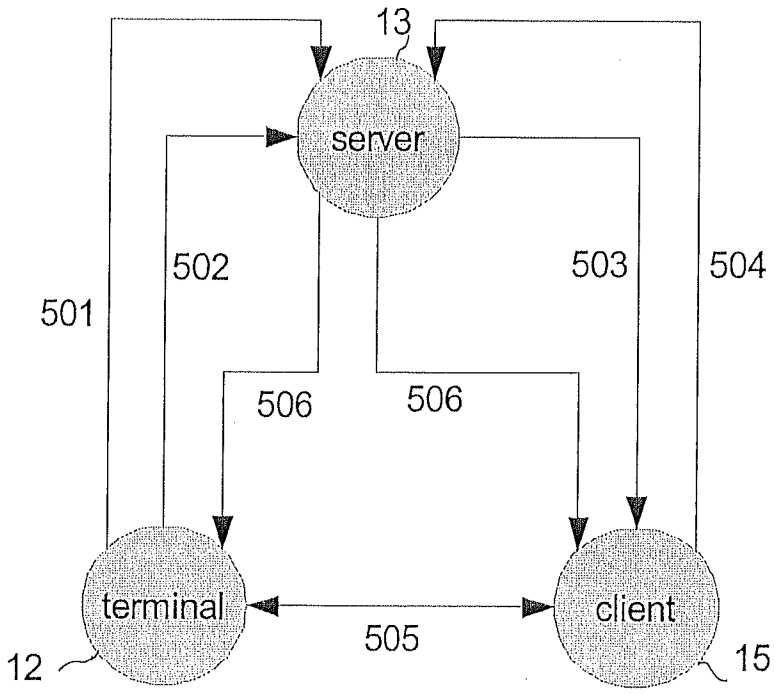

Fig. 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2014/052176

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q20/32 G06Q20/38
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)
G06Q

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 practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2011/258121 A1 (KAUNISKANGAS HANNU SAKARI [FI] ET AL) 20 October 2011 (2011-10-20)	1-4
Y	abstract paragraphs [0030] - [0038]; figure 1 paragraphs [0062] - [0067]; figure 6	5-10
Y	US 2011/270758 A1 (MIZANI OSKUI ALI [IR]) 3 November 2011 (2011-11-03) abstract	5-10
A	US 2013/151402 A1 (HOWARD LEE [US]) 13 June 2013 (2013-06-13) abstract paragraphs [0027] - [0046]; figure 2b	1-10

-/--

[X] Further documents are listed in the continuation of Box C.

[X] 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 application or patent 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	Date of mailing of the international search report
15 January 2015	21/01/2015

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Dedek, Frédéric

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2014/052176

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2013/159195 A1 (KIRILLIN VIACHESLAV [RU] ET AL) 20 June 2013 (2013-06-20) abstract paragraphs [0062] - [0066]; figure 5 -----	5-10

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2014/052176

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011258121 A1	20-10-2011	CN 102971758 A	13-03-2013
		EP 2558990 A1	20-02-2013
		US 2011258121 A1	20-10-2011
		WO 2011128499 A1	20-10-2011
US 2011270758 A1	03-11-2011	US 2011270758 A1	03-11-2011
		US 2011270764 A1	03-11-2011
US 2013151402 A1	13-06-2013	NONE	
US 2013159195 A1	20-06-2013	US 2013159195 A1	20-06-2013
		WO 2013089591 A1	20-06-2013

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2014/052176

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06Q20/32 G06Q20/38
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)
G06Q

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, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 2011/258121 A1 (KAUNISKANGAS HANNU SAKARI [FI] ET AL) 20 octobre 2011 (2011-10-20)	1-4
Y	abrégé alinéas [0030] - [0038]; figure 1 alinéas [0062] - [0067]; figure 6	5-10

Y	US 2011/270758 A1 (MIZANI OSKUI ALI [IR]) 3 novembre 2011 (2011-11-03) abrégé	5-10

A	US 2013/151402 A1 (HOWARD LEE [US]) 13 juin 2013 (2013-06-13) abrégé alinéas [0027] - [0046]; figure 2b	1-10

	-/--	

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] 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	Date d'expédition du présent rapport de recherche internationale
15 janvier 2015	21/01/2015

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Dedek, Frédéric

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2014/052176

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 2013/159195 A1 (KIRILLIN VIACHESLAV [RU] ET AL) 20 juin 2013 (2013-06-20) abrégé alinéas [0062] - [0066]; figure 5 -----	5-10

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2014/052176

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2011258121 A1	20-10-2011	CN 102971758 A	13-03-2013
		EP 2558990 A1	20-02-2013
		US 2011258121 A1	20-10-2011
		WO 2011128499 A1	20-10-2011
US 2011270758 A1	03-11-2011	US 2011270758 A1	03-11-2011
		US 2011270764 A1	03-11-2011
US 2013151402 A1	13-06-2013	AUCUN	
US 2013159195 A1	20-06-2013	US 2013159195 A1	20-06-2013
		WO 2013089591 A1	20-06-2013