(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
23 octobre 2014 (23.10.2014)

WIPO | PCT

(10) Numéro de publication internationale
WO 2014/170561 A1

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

(21) Numéro de la demande internationale :
PCT/FR2013/050888

(22) Date de dépôt international :
22 avril 2013 (22.04.2013)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
13 53407 15 avril 2013 (15.04.2013) FR

(71) Déposant : **BANQUE ACCORD** [FR/FR]; 40 avenue de Flandre, F-59170 Croix (FR).

(72) Inventeurs : **FELIN, Benoit**; 112 rue Emile Zola, F-59320 Hallennes-lez-Haubourdin (FR). **RIZET, Alexis**; 5 rue de Romainville, F-59300 Valenciennes (FR).

(74) Mandataire : **DEJADE ET BISET**; 35 rue Châteaudun, F-75009 Paris (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, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, 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, ML, MR, NE, SN, TD, TG).

Publiée :

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

(54) **Title** : METHOD AND SYSTEM FOR IMPROVING THE SECURITY OF ELECTRONIC TRANSACTIONS

(54) **Titre** : METHODE ET SYSTEME D'AMELIORATION DE LA SECURITE DES TRANSACTIONS ELECTRONIQUES

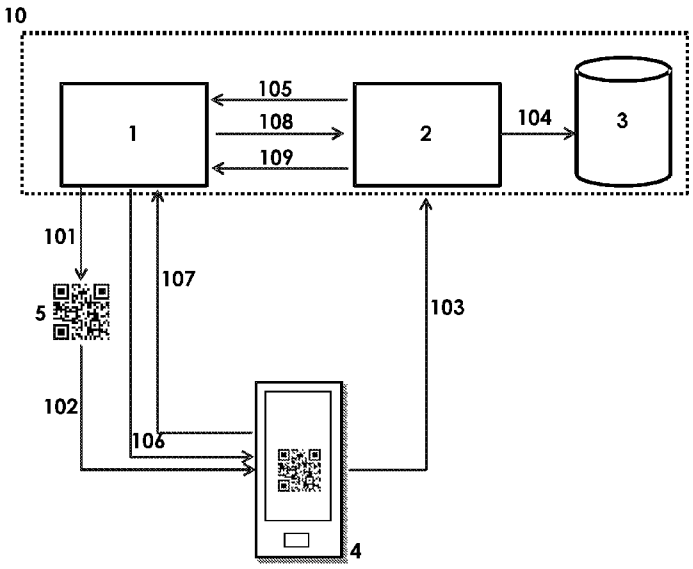


FIG.1

(57) **Abstract** : • - construction by the server (2) and the sale terminal (1) respectively of first and second encrypted messages; • - construction by the sale terminal (1) of a third encrypted message, using the second encrypted message, then transmission of same to the server (2); • - decryption by the server (2) of the third encrypted message, using the first encrypted message; • - construction by the server (2) of a fourth encrypted message on the basis of the content of the third decrypted message, using the first encrypted message, then transmission of same to the sale terminal (1); • - decryption by the sale terminal (1) of the fourth encrypted message, using the second encrypted message. • The sale terminal 1 generates and displays a set of information relative to the transaction in the form of a QR code 5, for example. This identification information will then be supplemented by a random chain consisting of a series of random characters, generated by the sale terminal 1. The decryption key is generated using two random numbers.

(57) **Abrégé** :

[Suite sur la page suivante]

WO 2014/170561 A1

• - la construction par le serveur (2) et le terminal de vente (1) respectivement d'un premier et deuxième message crypté; • - la construction par le terminal de vente (1) d'un troisième message chiffré en utilisant le deuxième message crypté, puis sa transmission au serveur (2); • - le déchiffrement par le serveur (2) du troisième message chiffré en utilisant le premier message crypté; • - la construction par le serveur (2) d'un quatrième message chiffré en fonction du contenu du troisième message déchiffré en utilisant le premier message crypté, puis sa transmission au terminal de vente (1); • - le déchiffrement par le terminal de vente (1) du quatrième message chiffré en utilisant le deuxième message crypté. • Le terminal de vente 1 génère et affiche un ensemble d'informations relatives à la transaction sous forme par exemple d'un code QR 5. Cette information d'identification va ensuite être complétée par une chaîne aléatoire composée d'une série de caractères aléatoires, générée par le terminal de vente 1. La clef de déchiffrement est générée en utilisant deux nombres aléatoires.

METHODE ET SYSTEME D'AMELIORATION DE LA SECURITE DES TRANSACTIONS ELECTRONIQUES

La présente invention a trait au domaine technique de la sécurisation des communications entre un terminal de vente et un serveur de contrôle de transaction.

On entend ci-après, par terminal de vente tout dispositif physique ou virtuel permettant d'effectuer une transaction électronique. A titre d'exemples non-exhaustifs on peut citer :

- comme terminaux de vente physiques : des bornes de vente de titres de transport pour des acteurs dans le domaine des transports (ferroviaire, aérien, maritime), des caisses enregistreuses sur des sites commerçants (pharmacies, restaurants), des caisses équipées d'un système de « self-checking » dans certains magasins (hypermarchés);
- comme terminaux de vente virtuels : des sites e-commerce proposant la vente de services et/ou de produits via un site web et/ou une application mobile dédiée.

Afin de pouvoir assurer les transactions, les gestionnaires des terminaux de vente sont amenés à déployer ou faire déployer lesdits terminaux sur des points de vente.

On entend ici par point de vente (ou *POS* en anglais pour « Point of Sale ») tout lieu physique ou virtuel proposant l'accomplissement de transaction, notamment la vente de produits (par exemples agroalimentaires, pharmaceutiques, multimédias) et/ou de services (par exemples livraisons, restauration, voyages, hôtellerie) indépendamment de sa taille ou de son domaine d'activité.

Suite à une demande de transaction initiée par un utilisateur sur un terminal de vente, ce terminal de vente peut être amené à effectuer un certain nombre de tâches afin de compléter cette transaction. Ces tâches consistent notamment à identifier et enregistrer des articles (produits ou/et services) à facturer à l'utilisateur, informer l'utilisateur concernant ladite transaction, et enfin gérer le paiement.

La tâche d'information de l'utilisateur concernant ladite transaction, consiste à titre d'exemple, à fournir à l'utilisateur un numéro identifiant la transaction, un numéro identifiant le terminal de vente utilisé par l'utilisateur, un récapitulatif de la liste des produits et/ou services concernés par la transaction, le montant à facturer à l'utilisateur ou encore le statut de la transaction.

L'ensemble des informations concernant la transaction peut être affiché selon différents modes : soit de manière virtuelle par exemple sur un écran d'une borne de paiement, soit de manière physique sur un support tel qu'un ticket de caisse.

Indépendamment du mode d'affichage (physique ou virtuel) des informations concernant la transaction, lesdites informations peuvent être affichées de différentes manières : par exemple sous forme textuelle, de code barre, de tag, de code QR (« Quick Response »), via un signal de type NFC ou plus généralement de tout type de codage d'informations.

Par ailleurs, afin de garantir aux utilisateurs un confort d'utilisation des terminaux de vente et donc un haut niveau de satisfaction, les terminaux de vente doivent pouvoir garantir le support des technologies les plus récentes. Parmi elles, on peut citer notamment le support du paiement mobile via un terminal mobile appartenant à l'utilisateur et/ou l'utilisation d'une application mobile installée sur le terminal mobile de l'utilisateur, afin d'interagir avec le terminal de vente préférentiellement via une interface sans-fil.

Par terminal mobile, on désigne ici notamment un téléphone mobile, un Smartphone, un PDA (personnal digital assistant) ou tout autre type de système de communication capable de récupérer les informations de transactions imprimées ou affichées par un terminal de vente et d'interagir avec un serveur distant.

On peut citer à titre d'exemple, le service de paiement à distance du stationnement de véhicule par terminal mobile, proposant via l'utilisation de différents terminaux de vente, un service de paiement à destinations de différentes catégories de terminaux utilisateur. Un automobiliste voulant payer un ticket de stationnement sélectionne une zone ou un tarif de

stationnement représenté par un code figurant sur les horodateurs ou sur internet, puis confirme le véhicule et la durée souhaitée. Cette solution fonctionne sur tout type de téléphones portables. Ainsi, il est possible d'accéder au service via un navigateur internet ou encore via une application Smartphone dédiée.

La figure 1 représente un système de vente **10**, comprenant un terminal de vente **1** et un serveur de contrôle de transaction **2** distant.

Par contrôle de transaction, on entend ici la gestion (à titre d'exemples réception, vérification, autorisation, validation) d'une liste d'informations transmises (par exemple identifiants, codes, statut de la transaction) associées à la transaction.

Dans l'état de la technique, le procédé mis en œuvre afin de mener une transaction entre un terminal de vente et un utilisateur muni d'un terminal mobile est le suivant.

Suite à une requête de transaction effectuée par un utilisateur muni d'un terminal mobile **4**, par exemple d'un Smartphone, le terminal de vente **1** génère et affiche un ensemble d'informations relatives à la transaction (interaction **101**) sous forme par exemple d'un code QR **5**.

L'utilisateur, à l'aide de son Smartphone **4**, capture le code QR **5** (interaction **102**) via une application dédiée.

Par application dédiée, on entend ici une application installée par l'utilisateur et répondant aux besoins d'un service spécifique. L'utilisateur peut être amené au préalable à souscrire audit service spécifique avant de pouvoir utiliser l'application dédiée correspondante. Ainsi à titre d'exemple, dans le cadre d'une application associée à un service de paiement, l'utilisateur devra au préalable souscrire audit service et fournir un certain nombre de données personnelles le concernant, par exemple ses identifiants bancaires. Suite à la souscription de l'utilisateur au service de paiement, l'application dédiée stockera alors sur le Smartphone une clef de chiffrement associée à la carte de paiement de l'utilisateur et une clé de chiffrement associée au code secret de l'utilisateur, en vue de leur future utilisation lors d'une transaction.

Il est entendu ici que l'utilisation d'un Smartphone et d'une application dédiée pour capturer un code QR est un exemple non-limitatif, et concerne de manière générale la capture d'informations de transaction par tout terminal mobile équipé d'un dispositif approprié.

Une fois le code QR capturé, le Smartphone **4** transmet au serveur de contrôle de transaction **2** distant le code QR capturé, des éléments d'identifications (par exemple des identifiants concernant le Smartphone et/ou l'utilisateur), la clef de déchiffrement de la carte de paiement de l'utilisateur ainsi que la clef de déchiffrement du code secret de l'utilisateur (interaction **103**).

Dès réception de ces données, le serveur de contrôle de transaction **2** identifie le terminal de vente **1** à l'aide du code QR. Il crée alors un identifiant de transaction et insère dans une base de données **3** un enregistrement (interaction **104**), contenant les éléments relatifs à la transaction (à titre d'exemple les identifiants du Smartphone **4** et du terminal de vente **1**) ainsi qu'un code relatif à l'état de la transaction.

Le serveur de contrôle de transaction **2** déchiffre ensuite les données de la carte de l'utilisateur à l'aide de la clef de déchiffrement correspondante transmise lors de l'interaction **103**, puis lance un processus mémoire en charge de scruter le code relatif à l'état de la transaction afin de déclencher une demande d'autorisation de transaction le moment venu.

Puis, le serveur de contrôle de transaction **2**, déchiffre le code secret de l'utilisateur à l'aide de la clef de déchiffrement correspondante transmise lors de l'interaction **103**, et génère une première chaîne aléatoire. Ladite première chaîne aléatoire est alors concaténée avec le code secret utilisateur, puis cryptée selon un premier algorithme de cryptographie. On obtient au final une chaîne de donnée cryptée nommée CSC (acronyme de Code Sécuritaire Crypté). La chaîne CSC obtenue (premier message crypté) est alors stockée dans la base de données **3** au niveau de la transaction (interaction **104**).

Ladite première chaîne aléatoire est par la suite transmise par le serveur de contrôle de transaction **2** au terminal de vente **1** en charge de la transaction avec l'utilisateur (interaction **105**).

A la réception de la première chaîne aléatoire, le terminal de vente **1** invite l'utilisateur à saisir son code secret (interaction **106**). Ce code secret est :

- soit supposé être le même que ledit code secret déchiffré par le serveur de contrôle de transaction **2**;
- soit de manière plus générale lié au code secret déchiffré par le serveur de contrôle de transaction **2**, c'est-à-dire qu'un code est déductible de l'autre en lui appliquant un procédé spécifique.

Après la saisie et validation du code secret par l'utilisateur (interaction **107**), le terminal de vente **1** concatène le code saisi avec ladite première chaîne aléatoire transmise par l'interaction **105**, puis applique le même type de cryptage, c'est-à-dire utilise le même dit premier algorithme de cryptographie que le serveur de contrôle de transaction **2**, afin de générer une chaîne CSC (deuxième message crypté) qu'on désignera par la suite par « CSC saisi ».

L'interaction **108** permet au terminal de vente **1** de communiquer le « CSC saisi » au serveur de contrôle de transaction **2**.

Le code secret utilisateur transmis au terminal de vente **1** étant supposé être le même que le (ou lié au) premier code secret décodé au niveau du serveur de contrôle de transaction **2**, le « CSC saisi» obtenu est donc supposé être le même que le CSC générée par le serveur de contrôle de transaction **2**.

Dès réception du « CSC saisi », le serveur de contrôle de transaction **2** compare le « CSC saisi » avec le CSC qu'il a lui-même généré et stocké dans la base de données **3**. Si ces deux éléments sont identiques, alors le code secret utilisateur transmis est correct et le serveur de contrôle de transaction **2** effectue alors l'autorisation et informe le terminal de vente **1** par l'interaction **109** qu'il peut clôturer la transaction. Dans le cas contraire, il informe le terminal de vente **1** par l'interaction **109** que le code saisi par l'utilisateur est erroné afin d'inviter l'utilisateur à de nouveau saisir son code (interactions **106** et **107**) et retransmettre ainsi un nouveau « CSC saisi » au serveur de contrôle de transaction **2** (interaction **108**).

L'avantage de ce procédé réside essentiellement dans le fait qu'un même code secret saisi lors de deux transactions différentes donne lieux à deux

chaînes cryptées (de type « CSC saisi ») différentes. Ceci permet de garantir l'impossibilité de trouver le code secret d'un utilisateur.

Cependant, une faille importante a été identifiée au cours de ce procédé le rendant vulnérable à une attaque connue couramment sous le nom de « Man in the Middle ». Celle-ci consiste à scruter/intercepter particulièrement l'interaction entre le serveur de contrôle de transaction **2** et le terminal de vente **1** (interactions **105**, **108** et **109**) puis simuler le serveur de contrôle de transaction **2** via l'interaction **109** en retournant systématiquement au terminal de vente **1** une réponse positive (ou négative) quel que soit le «CSC saisi » transmis par l'interaction **108**.

L'interaction **109** est particulièrement critique car celle-ci transmet la réponse finale du serveur de contrôle de transaction **2** : c'est à partir de la réponse transmise par cette interaction **109**, que le terminal de vente **1** valide/rejette et/ou clôture la transaction. Une des limites de l'état de la technique réside donc dans la vulnérabilité constatée pour l'interaction **109**, notamment si le protocole employé au cours de cette interaction est analysable et reproductible par un individu extérieur.

Une autre faille permet de procéder sur l'interaction **108,** à une attaque connue sous le nom d'« attaque par force brute ». Ce procédé consiste à tester de façon exhaustive toutes les combinaisons possibles de caractères, de manière à trouver au moins une information valide, ici le code secret de l'utilisateur.

Ainsi si un hacker dispose de l'algorithme de cryptographie utilisé par le terminal de vente **1** et parvient à intercepter l'interaction **108**, il lui sera possible via une méthode d'« attaque par force brute » de parvenir à identifier dans le « CSC saisi » le code secret de l'utilisateur.

Un objet de la présente invention est de pallier les inconvénients de l'art antérieur.

Un autre objet de la présente invention est de pouvoir améliorer la sécurisation des échanges entre un terminal de vente et un serveur de contrôle de transaction.

Dans ce but, l'invention se rapporte, selon un premier aspect, à une méthode de sécurisation des communications entre un terminal de vente et un serveur de contrôle de transaction, ladite méthode comprenant

- la construction, par le serveur de contrôle de transaction, selon un premier algorithme de cryptographie, d'un premier message crypté à partir d'au moins une première donnée;
- la construction, par le terminal de vente, selon le même dit premier algorithme de cryptographie, d'un deuxième message crypté à partir d'au moins une deuxième donnée, supposée être la même que la dite première donnée;

cette méthode comprenant en outre

- la construction, par ledit terminal de vente, selon un deuxième algorithme de chiffrement, d'un troisième message chiffré à partir d'au moins une troisième donnée, en utilisant ledit deuxième message crypté comme clef de chiffrement;
- la transmission, par ledit terminal de vente, dudit troisième message chiffré audit serveur de contrôle de transaction;
- le déchiffrement, par ledit serveur de contrôle de transaction, selon ledit deuxième algorithme de chiffrement, dudit troisième message chiffré, en utilisant ledit premier message crypté comme clé de déchiffrement;
- la construction, par ledit serveur de contrôle de transaction, selon un troisième algorithme de chiffrement, d'un quatrième message chiffré en fonction du contenu dudit troisième message déchiffré, en utilisant ledit premier message crypté comme clé de chiffrement;
- la transmission, par ledit serveur de contrôle de transaction, dudit quatrième message chiffré audit terminal de vente;
- le déchiffrement, par ledit terminal de vente, selon ledit troisième algorithme de chiffrement, dudit quatrième message chiffré, en utilisant ledit deuxième message crypté comme clé de déchiffrement.

L'invention se rapporte, selon un deuxième aspect, à un serveur de contrôle de transaction configuré pour

- construire selon un premier algorithme de cryptographie, un premier message crypté, à partir d'au moins une première donnée;
- réceptionner un deuxième message chiffré;

- déchiffrer selon un deuxième algorithme de chiffrement, ledit deuxième message chiffré, en utilisant ledit premier message crypté comme clé de déchiffrement;
- utiliser ledit premier message crypté comme clé de chiffrement, pour construire selon un troisième algorithme de chiffrement, un troisième message chiffré en fonction du contenu dudit deuxième message déchiffré;
- transmettre ledit troisième message chiffré.

L'invention se rapporte, selon un troisième aspect, à un terminal de vente configuré pour

- construire selon un premier algorithme de cryptographie, un premier message crypté, à partir d'au moins une première donnée;
- utiliser ledit premier message crypté comme clé de chiffrement, pour construire selon un deuxième algorithme de chiffrement, un deuxième message chiffré à partir d'au moins une deuxième donnée;
- transmettre ledit deuxième message chiffré;
- réceptionner un troisième message chiffré;
- déchiffrer selon un troisième algorithme de chiffrement, ledit troisième message chiffré, en utilisant ledit premier message crypté comme clé de déchiffrement;
- autoriser ou clôturer une transaction en fonction dudit troisième message déchiffré.

L'invention se rapporte, selon un quatrième aspect, à un système pour sécuriser des communications entre un terminal de vente et un serveur de contrôle de transaction, ledit système comprenant

- un serveur de contrôle de transaction configuré pour construire selon un premier algorithme de cryptographie, un premier message crypté, à partir d'au moins une première donnée;
- un terminal de vente configuré pour construire selon le même dit premier algorithme de cryptographie, un deuxième message crypté à partir d'au moins une deuxième donnée, supposée être la même que la dite première donnée;

ce système comprenant en outre

- le terminal de vente configuré pour construire selon un deuxième algorithme de chiffrement, un troisième message chiffré, à partir d'au

moins une troisième donnée, en utilisant ledit deuxième message crypté comme clef de chiffrement;

- le terminal de vente configuré pour transmettre ledit troisième message chiffré audit serveur de contrôle de transaction;
- le serveur de contrôle de transaction configuré pour déchiffrer selon ledit deuxième algorithme de chiffrement, ledit troisième message chiffré en utilisant ledit premier message crypté comme clé de déchiffrement;
- le serveur de contrôle de transaction configuré pour construire selon un troisième algorithme de chiffrement un quatrième message chiffré en fonction du contenu dudit troisième message chiffré, en utilisant ledit premier message crypté comme clé de chiffrement;
- le serveur de contrôle de transaction configuré pour transmettre ledit quatrième message chiffré audit terminal de vente;
- le terminal de vente configuré pour déchiffrer selon ledit troisième algorithme de chiffrement ledit quatrième message chiffré en utilisant ledit deuxième message crypté comme clé de déchiffrement.

L'invention se rapporte, selon un cinquième aspect, à un produit programme d'ordinateur implémenté sur un support mémoire, susceptible d'être mis en œuvre au sein d'une unité de traitement informatique et comprenant des instructions pour la mise en œuvre de la méthode résumée ci-dessus.

D'autres caractéristiques et avantages de l'invention apparaîtront plus clairement et de manière concrète à la lecture de la description ci-après de modes de réalisation préférés, laquelle est faite en référence à la figure 1 qui illustre schématiquement le contexte de mise en œuvre d'un mode de réalisation.

La présente invention propose d'enrichir le contenu du code QR **5** transmis par les interactions **101**, **102**,**103** et de modifier le contenu des échanges transmis par les interactions **108** et **109**.

Suite à une requête de transaction effectuée par un utilisateur muni d'un terminal mobile **4**, par exemple d'un Smartphone, le terminal de vente **1** génère et affiche un ensemble d'informations relatives à la transaction (interaction **101**) sous forme par exemple d'un code QR **5**.

L'ensemble des informations généré puis affiché comprend des informations relatives à la transaction, dont au moins une information d'identification fournie par le terminal de vente **1**.

D'une manière générale, l'information d'identification fournie par le terminal de vente **1**, consiste en toute information convenue au préalable entre le terminal de vente **1** et le serveur de contrôle de transaction **2**, ou encore toute autre information connue de part et d'autre.

A titre d'exemples, l'information d'identification fournie par le terminal de vente **1**, peut comprendre un jeton d'authentification et/ou une adresse IP connus du serveur de contrôle de transaction **2**.

Cette information d'identification va ensuite être complétée par une chaîne aléatoire composée d'une série de caractères aléatoires, générée par le terminal de vente **1**.

On désignera par la suite cette chaîne aléatoire par « deuxième chaine aléatoire », afin de la distinguer de la première chaîne aléatoire générée au niveau du serveur de contrôle de transaction **2**, lors de la construction du premier message crypté CSC.

Dans un mode de réalisation, le terminal de vente **1** génère et affiche un ensemble d'informations (interaction **101**) sous forme par exemple d'un code QR **5**, formé d'un jeton d'authentification connu du serveur de contrôle de transaction **2**, ledit jeton d'authentification étant complété par une série de caractères aléatoires générés par le terminal de vente **1**.

Le code QR **5**, et plus généralement l'ensemble des informations affiché par le terminal de vente **1** (interaction **101**), capturé par le terminal mobile **4** (interaction **102**) et transmis au serveur de contrôle de transaction **2** (interaction **103**) voit donc son contenu enrichi par la présence de la deuxième chaîne aléatoire ajoutée par le terminal de vente **1**.

A réception du code QR **5** le serveur de contrôle de transaction **2**, sépare le code QR **5** en deux parties:

- la partie contenant l'information supplémentaire, ici le jeton d'authentification qui va servir à identifier le terminal de vente;

- la partie contenant la deuxième chaîne aléatoire qui a été ajoutée par le terminal de vente **1**.

La construction d'un premier message crypté par le serveur de contrôle de transaction **2**, comprend:

- la génération d'une première chaîne aléatoire par le serveur de contrôle de transaction **2**;
- la concaténation du code secret utilisateur déchiffré avec ladite première chaîne aléatoire;
- l'utilisation d'un premier algorithme de cryptographie, afin de crypter la première chaîne aléatoire et le code secret concaténés.

Dans un mode de réalisation, la partie du code QR **5** contenant ladite deuxième chaîne aléatoire, va permettre de compléter la construction dudit premier message crypté :

Ladite première chaîne aléatoire générée par le par le serveur de contrôle de transaction **2**, est concaténée avec le code secret utilisateur, ensuite concaténée avec ladite deuxième chaîne aléatoire contenue dans le code QR **5**. La chaîne obtenue est enfin cryptée selon un premier algorithme de cryptographie. On obtient alors le premier message crypté correspondant au CSC.

De même, après la saisie et validation du code secret par l'utilisateur (interaction **107**), le terminal de vente **1** concatène le code saisi avec ladite première chaîne aléatoire transmise par l'interaction **105**, puis avec ladite deuxième chaîne aléatoire qu'il a généré. Il applique ensuite le même type de cryptage, c'est-à-dire utilise le même dit premier algorithme de cryptographie que le serveur de contrôle de transaction **2**, afin de générer le deuxième message crypté correspondant au « CSC saisi ».

Un avantage de l'utilisation d'une deuxième chaîne aléatoire pour la construction des CSC et « CSC saisi » (respectivement premier et deuxième message crypté) réside dans la complexité de ces messages. Plus particulièrement en termes d'effet technique, cela permet de renforcer l'entropie de ces messages : le nombre de combinaisons à tester pour une attaque de type « force brute » sur l'interaction **108** devient

particulièrement important. Ainsi même si un hacker dispose de l'algorithme de cryptographie employé pour la construction de ces messages, la présence de deux chaînes aléatoires rend un tel procédé très complexe à mettre en œuvre voire quasiment impossible, compte tenu du nombre de combinaisons à tester.

Comme autre avantage, on peut noter que contrairement à la première chaîne aléatoire transmise par l'interaction **105**, la deuxième chaîne aléatoire n'est pas transmise directement entre le serveur de contrôle de transaction **2** et le terminal de vente **1**. Ainsi même si un hacker parvenait à intercepter l'interaction **105** contenant la première chaîne aléatoire, et disposait de l'algorithme de cryptographie que le terminal de vente **1** utilise, la présence de ladite deuxième chaîne aléatoire limiterait le risque d'une attaque de type « force brute ».

Ledit « CSC saisi » est alors employé comme clef de chiffrement au cours d'un deuxième algorithme de chiffrement pour construire un nouveau message (troisième message chiffré). Ledit troisième message chiffré est constitué d'une chaîne aléatoire contenant elle-même l'identifiant du terminal de vente **1** à certaines positions connues du terminal de vente **1** et du serveur de contrôle de transaction **2**.

Ledit troisième message chiffré construit par le terminal de vente **1** est ensuite transmis (interaction **108**) au serveur de contrôle de transaction **2**.

Après réception dudit troisième message, le serveur de contrôle de transaction **2** utilise le CSC qu'il a stocké dans la base de données **3** comme clef de déchiffrement en se basant sur le même dit deuxième algorithme de chiffrement, pour déchiffrer le message reçu, en utilisant sa connaissance des positions de l'identifiant du terminal. Si l'identifiant du terminal de vente **1** est trouvé dans le message déchiffré alors le code secret saisi par l'utilisateur, transmis lors de l'interaction **107**, est correct. Dans le cas contraire, si l'identifiant du terminal de vente **1** n'est pas trouvé dans le message déchiffré, cela signifie que le « CSC saisi » diffère du CSC stocké dans la base de données **3**, le code saisi par l'utilisateur est donc incorrect.

Il est à noter ici que l'utilisation de l'identifiant du terminal de vente **1** pour la construction du troisième message chiffré, des positions dudit identifiant et sa reconnaissance lors du déchiffrement dudit troisième message chiffré, est donné à titre d'exemple non limitatif. De manière générale, il est possible d'utiliser toute autre information convenue au préalable entre le terminal de vente **1** et le serveur de contrôle de transaction **2**, ou encore toute autre information connue de part et d'autre. On peut citer comme autre information à titre d'exemple, l'adresse IP du terminal de vente **1**.

Le serveur de contrôle de transaction **2** génère alors en fonction du contenu dudit message déchiffré un message de contrôle. Ledit message de contrôle est constitué d'une chaîne aléatoire dans laquelle le serveur de contrôle de transaction **2** va placer à des positions connues du terminal de vente **1** et de lui même un code d'instruction de transaction, désigné ici par « code retour » de la transaction. A titre d'exemple le « code retour » est un message codé associé au statut de la transaction : « OK » si celle-ci est validée ou « KO » dans le cas contraire.

Ledit message de contrôle est ensuite chiffré à l'aide du CSC stocké dans la base de données **3** selon un troisième algorithme de chiffrement (obtention d'un quatrième message chiffré), puis transmis au point de vente **1** par l'interaction **109**.

A la réception dudit quatrième message chiffré, le point de vente **1** utilise le « CSC saisi » comme clef de déchiffrement en se basant sur le même dit troisième algorithme de chiffrement, pour déchiffrer ledit quatrième message chiffré. Ledit message déchiffré correspond ainsi audit message de contrôle. Le point de vente extrait alors dudit message de contrôle le « code retour » de la transaction en utilisant sa connaissance des positions dudit « code retour ».

Si ce « code retour » extrait est jugé cohérent par le terminal de vente **1**, cela signifie que le code secret saisi par l'utilisateur est correct. L'autorisation et/ou la clôture de transaction sont alors effectuées en fonction du contenu dudit « code retour ». A titre d'exemple on peut vérifier dans le « code retour » la présence d'un message codé associé au statut « OK » ou « KO» d'une transaction.

Dans le cas contraire l'utilisateur est invité à de nouveau saisir son code secret (interactions **106** et **107**) pour le retransmettre.

Par ailleurs en cas de saisie d'un code secret erroné par l'utilisateur, la probabilité que le « CSC saisi » puisse permettre de déchiffrer le message de contrôle (transmis par l'interaction **109**) afin d'en extraire un « code retour » cohérent, dépend de la longueur des informations à contrôler.

On peut citer à titre d'informations à contrôler, la longueur du « code retour » de transaction présent dans ledit message de contrôle.

Ainsi, dans un mode de réalisation, on convient de construire un « code retour » suffisamment long, afin de tendre vers une probabilité d'extraction d'un « code retour » cohérent quasi nulle, si le code secret de l'utilisateur est erroné.

Avantageusement, on peut compléter ce « code retour » lors de sa construction par des octets de contrôle de type CRC32.

Avantageusement un intrus écoutant les messages échangés entre le terminal de vente **1** et le serveur de contrôle de transaction **2** ne parvient pas à construire un message notifiant, par l'interaction **109**, au terminal de vente **1** qu'il peut clôturer favorablement (ou défavorablement) la transaction.

Un autre avantage de cette invention est que deux codes identiques saisis sur un même terminal de vente **1** donnent lieu à la construction de deux messages différents au cours de la même transaction, il est donc impossible pour un intrus d'analyser le protocole employé.

Avantageusement, la méthode qui vient d'être décrite permet :

- d'améliorer la sécurisation des transactions électroniques;
- de renforcer la sécurisation des échanges effectués entre un serveur de contrôle de transaction et un terminal de vente;
- d'améliorer le contenu des échanges entre un serveur de contrôle de transaction et un terminal de vente sans pour autant modifier leurs interactions respectives;
- d'empêcher toute analyse extérieure des protocoles utilisés;

- d'empêcher toute attaque de type « force brute »;
- de limiter tout risque d'attaques du type « Man in the Middle ».

REVENDICATIONS

1. Méthode de sécurisation des communications entre un terminal de vente (**1**) et un serveur de contrôle de transaction (**2**), ladite méthode comprenant

- la construction, par le serveur de contrôle de transaction (**2**), selon un premier algorithme de cryptographie, d'un premier message crypté à partir d'au moins une première donnée;
- la construction, par le terminal de vente (**1**), selon le même dit premier algorithme de cryptographie, d'un deuxième message crypté à partir d'au moins une deuxième donnée, supposée être la même que la dite première donnée;

cette méthode caractérisée en ce qu'elle comprend en outre

- la construction, par ledit terminal de vente (**1**), selon un deuxième algorithme de chiffrement, d'un troisième message chiffré à partir d'au moins une troisième donnée, en utilisant ledit deuxième message crypté comme clef de chiffrement;
- la transmission, par ledit terminal de vente (**1**), dudit troisième message chiffré audit serveur de contrôle de transaction (**2**);
- le déchiffrement, par ledit serveur de contrôle de transaction (**2**), selon ledit deuxième algorithme de chiffrement, dudit troisième message chiffré, en utilisant ledit premier message crypté comme clé de déchiffrement;
- la construction, par ledit serveur de contrôle de transaction (**2**), selon un troisième algorithme de chiffrement, d'un quatrième message chiffré en fonction du contenu dudit troisième message déchiffré, en utilisant ledit premier message crypté comme clé de chiffrement;
- la transmission, par ledit serveur de contrôle de transaction (**2**), dudit quatrième message chiffré audit terminal de vente (**1**);
- le déchiffrement, par ledit terminal de vente (**1**), selon ledit troisième algorithme de chiffrement, dudit quatrième message chiffré, en utilisant ledit deuxième message crypté comme clé de déchiffrement.

2. Méthode selon la revendication 1, comprenant en outre une étape d'autorisation ou de clôture d'une transaction, par ledit terminal de vente (**1**), en fonction dudit quatrième message déchiffré.

3. Méthode selon les revendications 1 ou 2, dans laquelle ladite troisième donnée comprend une chaîne aléatoire, contenant en des positions connues du terminal de vente (**1**) et du serveur de contrôle de transaction (**2**), une information convenue au préalable entre le terminal de vente (**1**) et le serveur de contrôle de transaction (**2**).
4. Méthode selon les revendications 1 ou 3, dans laquelle la construction dudit quatrième message chiffré, comprend le chiffrement d'une chaîne aléatoire, contenant en des positions connues du terminal de vente (**1**) et du serveur de contrôle de transaction (**2**), un code de retour de transaction.
5. Méthode selon la revendication précédente, dans laquelle ledit code retour est complété par des octets de contrôle lors de sa construction.
6. Méthode selon l'une quelconque des revendications 1 à 5, dans laquelle ladite première donnée et ladite deuxième donnée, correspondent à un code secret utilisateur.
7. Méthode selon l'une quelconque des revendications 1 à 6, dans laquelle ladite première donnée et ladite deuxième donnée comprennent une même chaîne aléatoire.
8. Serveur de contrôle de transaction (**2**) configuré pour :

– construire selon un premier algorithme de cryptographie, un premier message crypté, à partir d'au moins une première donnée;
– réceptionner un deuxième message chiffré;
– déchiffrer selon un deuxième algorithme de chiffrement, ledit deuxième message chiffré, en utilisant ledit premier message crypté comme clé de déchiffrement;
– utiliser ledit premier message crypté comme clé de chiffrement, pour construire selon un troisième algorithme de chiffrement, un troisième message chiffré en fonction du contenu dudit deuxième message déchiffré;
– transmettre ledit troisième message chiffré.

9. Terminal de vente (**1**) configuré pour

– construire selon un premier algorithme de cryptographie, un premier message crypté, à partir d'au moins une première donnée;
– utiliser ledit premier message crypté comme clé de chiffrement, pour construire selon un deuxième algorithme de chiffrement, un deuxième message chiffré à partir d'au moins une deuxième donnée;

- transmettre ledit deuxième message chiffré;
- réceptionner un troisième message chiffré;
- déchiffrer selon un troisième algorithme de chiffrement, ledit troisième message chiffré, en utilisant ledit premier message crypté comme clé de déchiffrement;
- autoriser ou clôturer une transaction en fonction dudit troisième message déchiffré.

10. Système pour sécuriser des communications entre un terminal de vente (**1**) et un serveur de contrôle de transaction (**2**), ledit système comprenant

- un serveur de contrôle de transaction (**2**) configuré pour construire selon un premier algorithme de cryptographie, un premier message crypté, à partir d'au moins une première donnée;
- un terminal de vente (**1**) configuré pour construire selon le même dit premier algorithme de cryptographie, un deuxième message crypté à partir d'au moins une deuxième donnée, supposée être la même que la dite première donnée;

ce système caractérisé en ce qu'il comprend en outre

- le terminal de vente (**1**) configuré pour construire selon un deuxième algorithme de chiffrement, un troisième message chiffré, à partir d'au moins une troisième donnée, en utilisant ledit deuxième message crypté comme clef de chiffrement;
- le terminal de vente (**1**) configuré pour transmettre ledit troisième message chiffré audit serveur de contrôle de transaction (**2**);
- le serveur de contrôle de transaction (**2**) configuré pour déchiffrer selon ledit deuxième algorithme de chiffrement, ledit troisième message chiffré en utilisant ledit premier message crypté comme clé de déchiffrement;
- le serveur de contrôle de transaction (**2**) configuré pour construire selon un troisième algorithme de chiffrement un quatrième message chiffré en fonction du contenu dudit troisième message chiffré, en utilisant ledit premier message crypté comme clé de chiffrement;
- le serveur de contrôle de transaction (**2**) configuré pour transmettre ledit quatrième message chiffré audit terminal de vente (**1**);
- le terminal de vente (**1**) configuré pour déchiffrer selon ledit troisième algorithme de chiffrement ledit quatrième message chiffré en utilisant ledit deuxième message crypté comme clé de déchiffrement.

11. Système selon la revendication précédente où le terminal de vente (**1**) est configuré en outre pour appliquer une étape d'autorisation ou de clôture de transaction en fonction dudit quatrième message déchiffré.

12. Produit programme d'ordinateur implémenté sur un support mémoire, susceptible d'être mis en œuvre au sein d'une unité de traitement informatique et comprenant des instructions pour la mise en œuvre d'une méthode selon l'une des revendications 1 à 7.

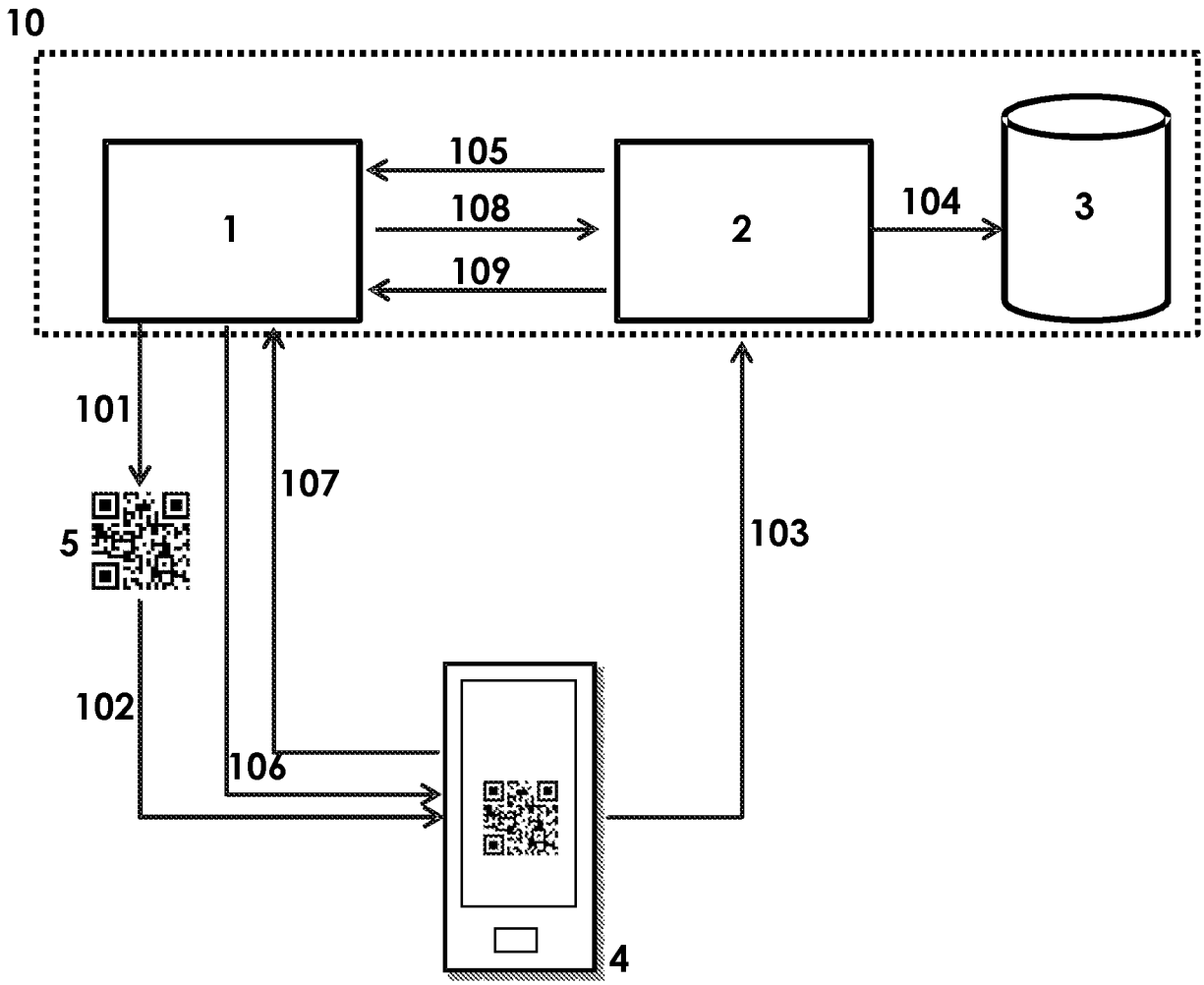


FIG.1

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2013/050888

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q20/38 G06Q20/20
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	CN 101 420 303 B (GCI SCIENCE & TECH CO LTD [CN] GCI SCIENCE & TECH CO LTD) 2 February 2011 (2011-02-02) abstract -----	1-12
X	JP 2012 050075 A (NIDEC COPAL CORP) 8 March 2012 (2012-03-08) abstract -----	1-12
X	WO 2010/067650 A1 (TOSHIBA KK [JP]; OHKUMA KENJI [JP]; MATSUSHITA TATSUYUKI [JP]; YAMANAK) 17 June 2010 (2010-06-17) paragraph [0018] -----	1-12
X	US 2006/013402 A1 (SUTTON JAMES A II [US] ET AL SUTTON II JAMES A [US] ET AL) 19 January 2006 (2006-01-19) paragraph [0048] -----	1-12
	-/--	

[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
7 January 2014	14/01/2014

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	Lavin Liermo, Jesus

3

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2009/138715 A1 (XIAO SHENG [US] ET AL) 28 May 2009 (2009-05-28) paragraph [0117]	1-12
X	CN 202 711 262 U (HANGZHOU SYNOCHIP TECHNOLOGIES CO LTD) 30 January 2013 (2013-01-30) abstract	1-12
X	US 2010/011213 A1 (HAMADA HIROAKI [JP] ET AL) 14 January 2010 (2010-01-14) paragraph [0128] - paragraph [0256]	1-12
X	EP 2 506 176 A1 (IRDETO CORPORATE B V [NL]) 3 October 2012 (2012-10-03) claim 7	1-12
X	US 2013/073850 A1 (ZAVERUCHA GREGORY MARC [CA]) 21 March 2013 (2013-03-21) abstract	1-12
A	KR 2012 0137093 A (UNIV KOREA RES & BUS FOUND [KR]) 20 December 2012 (2012-12-20) abstract	1
A	KR 2012 0134822 A (UNIV KOREA RES & BUS FOUND [KR]) 12 December 2012 (2012-12-12) figures 1-4	1
A	US 2011/099369 A1 (LEE CHUNG-I [TW] ET AL) 28 April 2011 (2011-04-28) paragraph [0020] - paragraph [0032]	1
A	EP 2 571 192 A1 (CERTICOM CORP [CA]) 20 March 2013 (2013-03-20) abstract	1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2013/050888

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
CN 101420303 B	02-02-2011	NONE	
JP 2012050075 A	08-03-2012	NONE	
WO 2010067650 A1	17-06-2010	JP 2010141408 A	24-06-2010
		WO 2010067650 A1	17-06-2010
US 2006013402 A1	19-01-2006	CN 101019369 A	15-08-2007
		DE 112005001672 B4	09-12-2010
		DE 112005001672 T5	31-05-2007
		GB 2430127 A	14-03-2007
		JP 4673890 B2	20-04-2011
		JP 2008507205 A	06-03-2008
		US 2006013402 A1	19-01-2006
		US 2010150351 A1	17-06-2010
		WO 2006023151 A2	02-03-2006
US 2009138715 A1	28-05-2009	NONE	
CN 202711262 U	30-01-2013	NONE	
US 2010011213 A1	14-01-2010	JP 4666240 B2	06-04-2011
		JP 2010045761 A	25-02-2010
		US 2010011213 A1	14-01-2010
		US 2013198515 A1	01-08-2013
EP 2506176 A1	03-10-2012	EP 2506176 A1	03-10-2012
		WO 2012130575 A1	04-10-2012
US 2013073850 A1	21-03-2013	NONE	
KR 20120137093 A	20-12-2012	NONE	
KR 20120134822 A	12-12-2012	NONE	
US 2011099369 A1	28-04-2011	CN 102231181 A	02-11-2011
		US 2011099369 A1	28-04-2011
EP 2571192 A1	20-03-2013	EP 2571192 A1	20-03-2013
		WO 2013039659 A1	21-03-2013

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2013/050888

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06Q20/38 G06Q20/20
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	CN 101 420 303 B (GCI SCIENCE & TECH CO LTD [CN] GCI SCIENCE & TECH CO LTD) 2 février 2011 (2011-02-02) abrégé	1-12
X	JP 2012 050075 A (NIDEC COPAL CORP) 8 mars 2012 (2012-03-08) abrégé	1-12
X	WO 2010/067650 A1 (TOSHIBA KK [JP]; OHKUMA KENJI [JP]; MATSUSHITA TATSUYUKI [JP]; YAMANAK) 17 juin 2010 (2010-06-17) alinéa [0018]	1-12
X	US 2006/013402 A1 (SUTTON JAMES A II [US] ET AL SUTTON II JAMES A [US] ET AL) 19 janvier 2006 (2006-01-19) alinéa [0048]	1-12

-/--

[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
7 janvier 2014	14/01/2014

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	Lavin Liermo, Jesus

3

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 2009/138715 A1 (XIAO SHENG [US] ET AL) 28 mai 2009 (2009-05-28) alinéa [0117]	1-12
X	CN 202 711 262 U (HANGZHOU SYNOCHIP TECHNOLOGIES CO LTD) 30 janvier 2013 (2013-01-30) abrégé	1-12
X	US 2010/011213 A1 (HAMADA HIROAKI [JP] ET AL) 14 janvier 2010 (2010-01-14) alinéa [0128] - alinéa [0256]	1-12
X	EP 2 506 176 A1 (IRDETO CORPORATE B V [NL]) 3 octobre 2012 (2012-10-03) revendication 7	1-12
X	US 2013/073850 A1 (ZAVERUCHA GREGORY MARC [CA]) 21 mars 2013 (2013-03-21) abrégé	1-12
A	KR 2012 0137093 A (UNIV KOREA RES & BUS FOUND [KR]) 20 décembre 2012 (2012-12-20) abrégé	1
A	KR 2012 0134822 A (UNIV KOREA RES & BUS FOUND [KR]) 12 décembre 2012 (2012-12-12) figures 1-4	1
A	US 2011/099369 A1 (LEE CHUNG-I [TW] ET AL) 28 avril 2011 (2011-04-28) alinéa [0020] - alinéa [0032]	1
A	EP 2 571 192 A1 (CERTICOM CORP [CA]) 20 mars 2013 (2013-03-20) abrégé	1

3

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2013/050888

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
CN 101420303 B	02-02-2011	AUCUN	
JP 2012050075 A	08-03-2012	AUCUN	
WO 2010067650 A1	17-06-2010	JP 2010141408 A	24-06-2010
		WO 2010067650 A1	17-06-2010
US 2006013402 A1	19-01-2006	CN 101019369 A	15-08-2007
		DE 112005001672 B4	09-12-2010
		DE 112005001672 T5	31-05-2007
		GB 2430127 A	14-03-2007
		JP 4673890 B2	20-04-2011
		JP 2008507205 A	06-03-2008
		US 2006013402 A1	19-01-2006
		US 2010150351 A1	17-06-2010
		WO 2006023151 A2	02-03-2006
US 2009138715 A1	28-05-2009	AUCUN	
CN 202711262 U	30-01-2013	AUCUN	
US 2010011213 A1	14-01-2010	JP 4666240 B2	06-04-2011
		JP 2010045761 A	25-02-2010
		US 2010011213 A1	14-01-2010
		US 2013198515 A1	01-08-2013
EP 2506176 A1	03-10-2012	EP 2506176 A1	03-10-2012
		WO 2012130575 A1	04-10-2012
US 2013073850 A1	21-03-2013	AUCUN	
KR 20120137093 A	20-12-2012	AUCUN	
KR 20120134822 A	12-12-2012	AUCUN	
US 2011099369 A1	28-04-2011	CN 102231181 A	02-11-2011
		US 2011099369 A1	28-04-2011
EP 2571192 A1	20-03-2013	EP 2571192 A1	20-03-2013
		WO 2013039659 A1	21-03-2013