(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
08 février 2018 (08.02.2018)

WIPO | PCT

(10) Numéro de publication internationale
WO 2018/024980 A1

(51) Classification internationale des brevets :
G06Q 20/02 (2012.01) *G06Q 20/34* (2012.01)
G06Q 20/20 (2012.01) *G06Q 20/36* (2012.01)
G06Q 20/32 (2012.01) *G06Q 20/40* (2012.01)

(21) Numéro de la demande internationale :
PCT/FR2017/052156

(22) Date de dépôt international :
31 juillet 2017 (31.07.2017)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1657474 01 août 2016 (01.08.2016) FR

(71) Déposant : **ORANGE** [FR/FR] ; 78 RUE OLIVIER DE SERRES, 75015 PARIS (FR).

(72) Inventeurs : **BELLEE, Arnaud** ; 13 bis rue du Four, 14790 Fontaine Etoupefour (FR). **BURGER, Jacques** ; 7, Haute Rue, 14112 BIEVILLE BEUVILLE (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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,

(54) **Title:** METHOD FOR IMPLEMENTING A TRANSACTION FROM AN ELECTRONIC TRANSACTION MEANS

(54) **Titre :** PROCÉDÉ DE MISE EN ŒUVRE D'UNE TRANSACTION DEPUIS UN MOYEN DE TRANSACTION ÉLECTRONIQUE

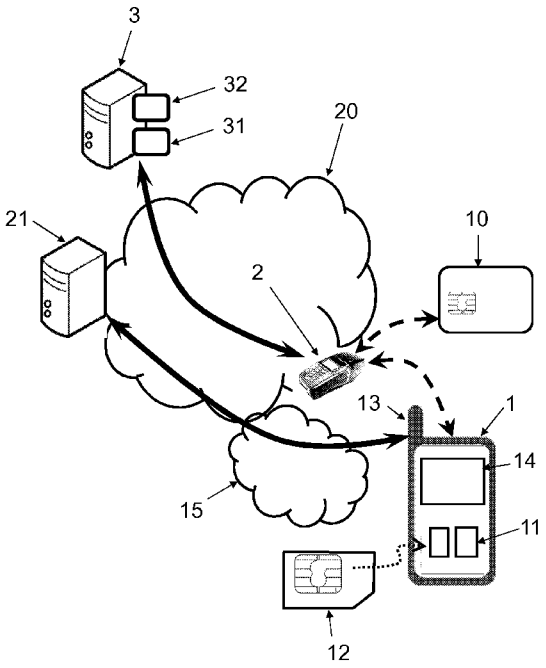

FIG. 1

(57) Abstract: The present invention relates to a method for implementing a transaction from an electronic transaction means (1, 10) of a user, on which is stored at least one transaction module capable of authorising a transaction when it is activated, the electronic transaction means (1, 10) further comprising a communication unit (13) for communicating with a network (20); the method being characterised in that it comprises implementing by the electronic payment means (1, 10) of steps of: (a) obtaining from a server (21) of the network (20) via the communication unit (13), a list of identifiers of beneficiaries of recurring transactions; (b) receiving a transaction request intended for said transaction module, the request comprising at least one amount of said transaction and an identifier of the beneficiary of said transaction; (c) determining an authentication procedure of the user of the electronic payment means (1, 10) from a plurality of procedures depending on the amount and identifier of the beneficiary of said received transaction, and on the list of identifiers of beneficiaries of recurring transactions; (d) if said determined authentication procedure is completed, activating said transaction module, and sending a transaction authorisation in response to said transaction request.

(57) Abrégé : La présente invention concerne un procédé de mise en œuvre d'une transaction depuis un moyen de transaction électronique (1, 10) d'un utilisateur, sur lequel est stocké au moins un module de transaction adapté pour autoriser une transaction lorsqu'il est activé, le moyen de transaction électronique (1, 10) comprenant en outre une unité de communication (13) avec un réseau (20); Le procédé étant caractérisé en ce qu'il comprend la mise en œuvre par le moyen de paiement électronique (1, 10) d'étapes de : (a) Obtention depuis un serveur (21) du réseau (20) via l'unité de communication (13)

WO 2018/024980 A1

[Suite sur la page suivante]

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))*

d'une liste d'identifiants de bénéficiaires de transactions récurrents; (b) réception d'une requête de transaction visant ledit module de transaction, la requête comprenant au moins un montant de ladite transaction et un identifiant du bénéficiaire de ladite transaction; (c) Détermination d'une procédure d'authentification de l'utilisateur du moyen de paiement électronique (1, 10) parmi une pluralité de procédure en fonction desdits montant et identifiant du bénéficiaire de ladite transaction reçus, et de ladite liste d'identifiants de bénéficiaires de transactions récurrents; (d) Si ladite procédure d'authentification déterminée est complétée, activation dudit module de transaction, et émission d'une autorisation de transaction en réponse à ladite requête de transaction.

Procédé de mise en œuvre d'une transaction depuis un moyen de transaction électronique

DOMAINE TECHNIQUE GENERAL

La présente invention concerne le domaine des transactions au moyen de terminaux mobiles ou cartes électroniques.

Plus précisément, elle concerne un procédé pour la mise en œuvre d'une transaction depuis un moyen de transaction électronique d'un utilisateur.

ETAT DE L'ART

Il est aujourd'hui possible de procéder à une transaction au niveau d'une borne de paiement via une carte bancaire physique ou dématérialisée (ou « virtualisés ») c'est-à-dire simulée par un support électronique, par exemple un terminal mobile.

Dans une cas comme dans l'autre, il est prévu pour des petits montants (moins de 20€, seuil dit « de régulation ») d'éviter la saisie d'un code de carte bancaire (le PIN bancaire) notamment en mettant en œuvre un paiement sans contact avec une borne de paiement par exemple de type NFC. Cela permet de diminuer fortement les manipulations et le temps nécessaire à la transaction car l'utilisateur n'a qu'à approcher sa carte ou son smartphone de la borne pour payer, et donc d'éviter aux consommateurs de faire la queue aux caisses.

Aujourd'hui, le seuil de régulation pour le paiement sans code PIN est bas et fixée de façon globale par les banques de sorte à éviter des fraudes. Le remonter augmenterait le nombre de transaction éligibles et permettrait de gagner du temps, mais provoquerait mathématiquement plus de fraude au vu des sommes plus importantes gagnables.

Le document US 2016/132880 A1 décrit des règles relatives à l'autorisation des transactions de paiement sans contact. Après la fourniture d'informations de paiement sans contact à un marchand, l'appareil mobile reçoit une requête relative à l'autorisation de la transaction. Les détails de la transaction figurant dans la requête sont comparés aux règles stockées sur l'appareil mobile. Au nombre de ces règles, certains marchands peuvent être spécifiés, pour

lesquels le seuil de régulation ne s'applique pas. Cependant ce système ne permet pas de s'affranchir du risque de fraude et la manière de sélectionner des marchands reste problématique.

Il serait par conséquent souhaitable de disposer d'une nouvelle solution de paiement par terminal qui soit plus ergonomique mais tout aussi sécurisée.

PRESENTATION DE L'INVENTION

La présente invention se rapporte ainsi selon un premier aspect à un procédé de mise en œuvre d'une transaction depuis un moyen de transaction électronique d'un utilisateur, sur lequel est stocké au moins un module de transaction adapté pour autoriser une transaction lorsqu'il est activé, le moyen de transaction électronique comprenant en outre une unité de communication avec un réseau ;

Le procédé étant caractérisé en ce qu'il comprend la mise en œuvre par le moyen de paiement électronique d'étapes de :

(a) Obtention depuis un serveur du réseau via l'unité de communication d'une liste d'identifiants de bénéficiaires de transactions récurrents ;

(b) réception d'une requête de transaction visant ledit module de transaction, la requête comprenant au moins un montant de ladite transaction et un identifiant du bénéficiaire de ladite transaction ;

(c) Détermination d'une procédure d'authentification de l'utilisateur du moyen de paiement électronique parmi une pluralité de procédure en fonction desdits montant et identifiant du bénéficiaire de ladite transaction reçus, et de ladite liste d'identifiants de bénéficiaires de transactions récurrents ;

(d) Si ladite procédure d'authentification déterminée est complétée, activation dudit module de transaction, et émission d'une autorisation de transaction en réponse à ladite requête de transaction.

(e)

L'utilisation d'un historique de transactions couplée à une détermination (en particulier par un élément de sécurité) d'une procédure de transaction à prévoir permet de contourner le seuil de régulation de paiement sans code PIN, de sorte à augmenter virtuellement ce seuil chez des marchands récurrents avec lesquels l'utilisateur a une relation de confiance.

Cela augmente le nombre de transaction rapides possibles, et facilite la vie de tout le monde sans diminuer la sécurité.

Selon d'autres caractéristiques avantageuses et non limitatives :

- le moyen de transaction électronique est choisi parmi une carte électronique physique et un terminal mobile sur lequel ledit module de transaction est associé à une carte électronique, et adapté pour autoriser une transaction pour le compte de ladite carte électronique lorsqu'il est activé ;
- le moyen de transaction électronique est un terminal mobile comprenant un module de traitement de données et un élément de sécurité sur lequel est stocké ledit module de transaction ;
- l'élément de sécurité est soit un élément matériel choisi parmi une carte d'identification d'abonné et un espace d'exécution sécurisé du module de traitement de données du terminal, soit un élément logiciel émulé par le module de traitement de données du terminal conformément à l'architecture Emulation de Cartes Hébergées, HCE ;
- l'élément de sécurité met en œuvre ledit module de transaction et un module de risque stockant ladite liste d'identifiants de bénéficiaires de transactions récurrents, et le module de traitement de données met en œuvre un module de gestion du ou des modules de transaction, l'étape (b) comprenant l'interrogation du module de risque par le module de transaction visé ;
- l'étape (a) comprend la réception par le module de gestion de données d'historique représentatives de transactions précédentes, la génération de ladite liste d'identifiants de bénéficiaires de transactions récurrents par le module de gestion à partir desdites données d'historique représentatives de transactions précédentes, et la transmission de ladite liste au module de risque ;
- le moyen de transaction électronique est un moyen de paiement électronique, la requête de transaction étant reçue à l'étape (a) depuis un terminal de paiement électronique en communication sans fil avec le moyen de paiement électronique, l'autorisation de transaction étant émise à l'étape (d) à destination du terminal de paiement électronique ;
- le procédé comprend en outre une étape (e) de transmission de l'autorisation de transaction à un serveur bancaire associé à ladite carte bancaire via le réseau ;

- ladite procédure d'authentification de l'utilisateur du moyen de paiement électronique est déterminée entre une procédure normale et une procédure simplifiée ;
- ladite procédure normale comprend la vérification d'un code confidentiel saisi par l'utilisateur et/ou la vérification d'un paramètre biométrique de l'utilisateur, et la procédure simplifiée ne comprend ni vérification d'un code confidentiel saisi par l'utilisateur, ni vérification d'un paramètre biométrique de l'utilisateur ;
- l'étape (d) comprend en cas de procédure normale l'émission par le module de transaction visé, à destination du module de gestion, d'une requête de présentation d'un code confidentiel associé au module de transaction, le module de gestion étant configuré pour requérir et obtenir via une interface du terminal ledit code confidentiel ;
- chaque identifiant de bénéficiaire de transaction récurrent de ladite liste est associé à un seuil, l'étape (c) comprenant :
  - Si ledit identifiant reçu du bénéficiaire de la transaction appartient à ladite liste, la procédure d'authentification de l'utilisateur du moyen de paiement électronique est déterminée comme étant la procédure simplifiée si le montant de transaction reçu est inférieur ou égal au seuil associé dans la liste à l'identifiant reçu ;
- un seuil par défaut est stocké dans le moyen de transaction électronique, chaque seuil de ladite liste étant supérieur au seuil par défaut, l'étape (c) comprenant :
  - Si ledit identifiant reçu du bénéficiaire de la transaction n'appartient à ladite liste, la procédure d'authentification de l'utilisateur du moyen de paiement électronique est déterminée comme étant la procédure simplifiée si le montant de transaction reçu est inférieur ou égal au seuil par défaut ;
- le procédé comprend une étape (e) de notification de la transaction autorisée au serveur de sorte à mettre à jour ladite liste d'identifiants de bénéficiaires de transactions récurrents.

Selon un deuxième aspect, l'invention concerne un moyen de transaction électronique sur lequel est stocké au moins un module de transaction adapté pour autoriser une transaction lorsqu'il est activé, et comprenant une unité de communication avec un réseau,

Le moyen de transaction électronique étant configuré pour :

- Obtenir depuis un serveur du réseau via l'unité de communication une liste d'identifiants de bénéficiaires de transactions récurrents ;
- recevoir une requête de transaction visant ledit module de transaction, la requête comprenant au moins un montant de ladite transaction et un identifiant du bénéficiaire de ladite transaction ;
- déterminer une procédure d'authentification de l'utilisateur du moyen de paiement électronique parmi une pluralité de procédure en fonction desdits montant et identifiant du bénéficiaire de ladite transaction reçus, et de ladite liste d'identifiants de bénéficiaires de transactions récurrents ;
- Si ladite procédure d'authentification déterminée est complétée, activer ledit module de transaction, et émettre une autorisation de transaction en réponse à ladite requête de transaction

Selon d'autres caractéristiques avantageuses et non limitatives le moyen de transaction électronique est un terminal mobile, le module de transaction étant associé à une carte électronique, et adapté pour autoriser une transaction pour le compte de ladite carte électronique lorsqu'il est activé.

Selon un troisième aspect, l'invention concerne un produit programme d'ordinateur comprenant des instructions de code pour l'exécution d'un procédé selon le premier aspect de l'invention de mise en œuvre d'une transaction depuis un moyen de transaction électronique d'un utilisateur.

Selon un quatrième aspect, l'invention concerne un moyen de stockage lisible par un équipement informatique sur lequel on trouve ce produit programme d'ordinateur.

PRESENTATION DES FIGURES

D'autres caractéristiques et avantages de la présente invention apparaîtront à la lecture de la description qui va suivre d'un mode de réalisation préférentiel. Cette description sera donnée en référence aux dessins annexés dans lesquels :

- la figure 1 est un schéma d'une architecture générale de réseau pour la mise en œuvre de l'invention ;

- les figures 2a-2c représentent trois modes de réalisation de mise en œuvre d'une transaction via le procédé selon l'invention.

DESCRIPTION DETAILLEE

Principe

Comme expliqué auparavant, la limite de montant pour le paiement sans code PIN (de façon générale sans autre authentification autre que la possession du moyen de transaction électronique) ne peut être augmentée de façon globale sous peine d'encourager la fraude, mais on comprend qu'il serait intéressant de s'en affranchir dans le cas de marchands chez lesquels l'utilisateur vient régulièrement consommer.

Par exemple, l'utilisateur vient généralement toujours faire ses courses quotidiennes dans les mêmes magasins, et une assurance peut être apportée par la récurrence et la proximité. En d'autres termes, on peut supposer avec un très haut niveau de certitude que l'utilisateur qui a payé au même endroit un grand nombre de fois avec la même carte bancaire est de confiance, ce qui n'est pas le cas si c'est dans un lieu nouveau et éloigné. Cette technique est par exemple utilisée dans la demande EP3014542 pour vérifier une cohérence entre le lieu courant et lesdites localisations précédentes du terminal, et le cas échéant détecter des transactions frauduleuses.

Lorsque sont identifiés des utilisateurs de confiance, il serait intéressant de relever le seuil de régulation, i.e. de faciliter des « procédures simplifiées » sans authentification de l'utilisateur, de sorte à diminuer le temps de paiement de ces utilisateurs et ainsi le temps d'attente global dans les points de vente, surtout que ces transactions « de confiance » constituent une grosse partie si ce n'est la majorité des transactions.

Pour pouvoir identifier ces utilisateurs de confiance et définir si une procédure simplifiée peut être utilisée, la présente invention propose une solution qui se démarque des procédés connus en utilisant non pas la géolocalisation, mais un historique de transaction passées, des règles définies par apprentissage sur cette base, et une architecture particulière pour appliquer ses règles sans attenter à la sécurité.

Architecture

En référence à la **figure 1**, l'invention propose un procédé pour la mise en œuvre d'une transaction depuis un moyen de transaction électronique 1, 10 d'un utilisateur. Par moyen de transaction électronique, on entend soit une carte électronique physique 10 (typiquement une carte bancaire, on verra plus de détail à ce sujet plus loin), soit un terminal mobile 1.

Dans tous les cas, le moyen 1, 10 stocke au moins un module de transaction adapté pour autoriser une transaction lorsqu'il est activé

A ce titre, la transaction est mise en œuvre soit directement en utilisant la carte électronique physique 10, soit en utilisant une telle carte dématérialisée sur le terminal 1, i.e. en reproduisant l'utilisation d'une carte électronique 10. Dans ce dernier cas, ledit module de transaction est associé à une carte électronique, et adapté pour autoriser une transaction pour le compte de ladite carte électronique lorsqu'il est activé.

La transaction est typiquement une transaction de paiement (c'est-à-dire que la carte physique 10 ou dématérialisée sur le terminal 1 est une carte bancaire), en particulier une transaction de proximité initiée par un terminal de paiement électronique (TPE) 2 tel que l'on trouve dans la plupart des points de vente (par exemple de type EFTPOS). Les TPE possèdent en effet pour la plupart des moyens de communication en champ proche (NFC) destinés à interagir avec une carte bancaire physique 10 disposant de cette technologie, mais leur permettant également d'interagir avec un terminal mobile 1.

De façon générale, dans le cas de transactions de paiement, un module de transaction (appelé alors « token ») contient (entre autres) un identifiant de la carte dématérialisée, le cas échéant un code supplémentaire (par exemple le cryptogramme visuel), et un code confidentiel (le code PIN de la carte dématérialisée). A noter qu'un terminal 1 peut stocker une pluralité de modules de transaction de sorte à simuler plusieurs cartes électroniques.

On comprendra néanmoins que le présent procédé n'est pas limité à des transactions de paiement, mais peut concerner toute transaction utilisant une carte physique 10 ou reproduite sur un terminal 1, et notamment des télétransmissions de feuilles de soins via Carte Vitale, des validations d'actes médicaux via Carte de Professionnel de Santé, etc., à condition que la transaction soit associée à un montant de ladite transaction et un identifiant du bénéficiaire de ladite transaction

Dans la suite de la présente demande, on prendra l'exemple de la transaction de paiement, et l'homme du métier saura transposer à d'autres applications.

Le moyen de transaction électronique 1, 10 comprend en outre une unité de communication 13 avec un réseau 20 (par exemple Internet), en vue de communiquer avec un serveur de contrôle 21 du réseau 20. Dans le cas où le moyen de transaction électronique est un terminal mobile 1, il s'agit tout simplement d'une unité de communication sans fil avec un réseau mobile 15 (3G, 4G, Wi-Fi, etc.) lui-même connecté au réseau 20. La connexion via cette unité 13 est alors distincte de celle en champ proche (connexion sans-fil de proximité, en général NFC, mais aussi Wi-Fi ou Bluetooth) que le terminal 1 peut avoir avec un TPE 2 (il est tout à fait possible que les deux connexions soient actives simultanément). Dans le cas d'une carte électronique physique 10, soit cette carte est une carte avancée disposant d'une unité de communication du même type que celle d'un terminal mobile, soit l'unité 13 est confondue avec les moyen de communications en champ proche, et alors le TPE 2 est configuré de sorte à permettre à la carte 10 certaines connexions particulières avec le réseau 20.

En fonctionnement, le TPE 2 est dans tous les cas d'une part connecté via une liaison sans-fil (NFC, mais aussi Wi-Fi ou Bluetooth) au moyen de transaction électronique 1, 10, et d'autre part connecté à au moins un serveur bancaire 3 via le réseau 20, mais en général l'accès du TPE 2 au réseau 20 est restreint, de sorte que le TPE ne puisse pas avoir accès à d'autres équipements que les serveurs bancaires 3 et réciproquement.

Dans le mode de réalisation particulier où le moyen de transaction est une carte physique 10 qui n'a pas d'unité de communication 13 autre que celle adaptée pour communiquer en champ proche avec le TPE 2, ce dernier est configuré de sorte à autoriser une communication avec le serveur de contrôle 21 du réseau 20, en plus de la communication avec les serveurs bancaires 3. On comprendra que dans mode de réalisation, le TPE 2 reste limité à des connexions aux serveurs bancaires 3 et au serveur de contrôle 20 de sorte à éviter des failles de sécurité.

Dans le cas où le moyen de transaction électronique est un terminal mobile 1, ce dernier peut être de n'importe quel type, en particulier smartphone ou des tablettes tactiles. Il comprend un module de traitement de données 11 (un processeur), un module de stockage de données (une mémoire), une interface

utilisateur (IHM) 14 comprenant par exemple des moyens de saisie et des moyens d'affichage (par exemple un écran tactile).

Le terminal 1 comprend en outre avantageusement un élément de sécurité 12 pour le stockage dudit module de transaction. De façon préférée, il s'agit d'un élément adapté pour autoriser une connexion du terminal 1 à un réseau de communication mobile, en particulier une carte d'identification d'abonné. Par « carte d'identification d'abonné », on entend tout circuit intégré capable d'assurer les fonctions d'identification d'un abonné à un réseau via des données qui y sont stockées, et tout particulièrement une carte « SIM » (de l'anglais « Subscriber Identity Module »), ou une carte « e-UICC » (pour « (embedded)-Universal Integrated Circuit Card ») comprenant des moyens de traitement de données sous la forme d'un microcontrôleur et de la mémoire de type « EEPROM » (pour « Electrically-Erasable Programmable Read-Only Memory »), ou flash. L'invention n'est pas limitée à ce type d'élément de sécurité. Ainsi, dans un autre exemple de réalisation, l'élément de sécurité 12 est une zone mémoire sécurisée du terminal mobile tel un composant « TEE » (de l'anglais « Trusted Execution Environment ») embarqué dans le module de traitement de données 11, ou un élément matériel dédié du terminal 1 (par exemple un microcontrôleur, une puce « eSE » pour « (embedded)-Secure Element » ou n'importe quel « Secure Component GP (GlobalPlatform) »), voire un composant amovible de type microSD (« SD » pour Secure Digital).

Alternativement à un élément de sécurité 12 « physique », le module de traitement de données 11 (processeur « non-sécurisé ») peut avoir une fonctionnalité dite d'Emulation de Cartes Hébergées, ou HCE (Host Card Emulation), qui lui permet « d'émuler » un élément de sécurité, et de gérer directement et de façon sécurisée le module de transaction. Dans un tel mode de réalisation, on comprendra que le terminal mobile 1 comprend malgré tout un élément de sécurité 12, mais qu'il est purement logiciel.

Dans tous les cas, le module de traitement de données 11 du terminal 1 met quant à lui en œuvre de façon préférée un module de gestion de type « wallet », i.e. une application de portefeuille électronique. Si l'utilisateur souhaite utiliser l'une de ses cartes électroniques dématérialisées pour une transaction, il lui suffit d'ouvrir le wallet comme seule application de paiement, et ce dernier lui propose de choisir entre les cartes (et plus particulièrement entre les modules de transactions des cartes) celle qu'il souhaite utiliser, il n'a plus qu'à saisir (si

nécessaire, voir plus loin) le code PIN associé. Les wallets permettent également des fonctions supplémentaires telles que le changement de code PIN.

Ce wallet peut être astucieusement complété par un « wallet companion », i.e. un module d'authentification tel que décrit dans la demande FR1562797.

Le serveur bancaire 3 du réseau 20 désigne une plateforme de gestion des transactions, et comprend un module de traitement de données 31, par exemple un processeur et un module de stockage de données 32 tel qu'un disque dur ou de façon préférée un HSM (pour « Hardware Security Module »).

On comprendra que la notion de « serveur 3 » peut englober une pluralité de serveurs bancaires distincts connectés et adaptés pour communiquer ensemble.

Le serveur de contrôle 21 est quant à lui typiquement un serveur d'un opérateur des moyens de transaction électronique 1, 10 et va permettre comme l'on va voir de faire remonter des données de contrôle des transactions. Il peut y en avoir plusieurs, et particulier un par type de moyen 1, 10 et/ou un par réseau de paiement.

Procédé de mise en œuvre de la transaction

En référence aux **figures 2a-c** vont être décrits trois exemples de réalisation du présent procédé selon l'invention. On comprendra que ces exemples ne sont qu'illustratifs. Dans les figures 2a et 2b, on est dans le cas d'un terminal 1 présentant un élément de sécurité 12 distinct de type carte SIM, et dans la figure 2c on est dans le cas où il n'y a pas d'élément de sécurité distinct, ce qui est typiquement le cas d'un terminal mobile 1 dit HCE (Host Card Emulation), où l'élément de sécurité est émulé par le module traitement de données 11 (on considèrera qu'il y a toujours un élément de sécurité 12, mais qu'il est fait partie du module de traitement 11). La situation sera similaire dans le cas où le moyen de paiement est une carte électronique physique 10, puisque le microprocesseur d'une carte électronique physique 10 est par définition un élément de sécurité.

Dans la suite de la description, on prendra l'exemple préféré de la transaction au moyen d'un terminal mobile 1, mais on décrira par la suite comme adapter le présent procédé à d'autres moyens de transaction électronique et en particulier une carte physique 10.

Dans une première étape (a), le terminal 1 (et plus précisément un module de risque stocké dans l'élément de sécurité 12) obtient (directement ou indirectement) depuis le serveur de contrôle 21 du réseau 20 via l'unité de communication 13 (typiquement via un réseau mobile 15 dans le cas du terminal 1) une liste d'identifiants de bénéficiaires de transactions récurrents.

Cette liste, construite par apprentissage, est générée soit par le module de traitement de données 11 du terminal 1 (plus précisément par le wallet) à partir de données d'historique représentatives des transactions précédentes fournies par le serveur 21 (cas des figures 2a et 2c, on comprend alors qu'elle est obtenue indirectement), soit directement par le serveur 21 (cas de la figure 2b. A noter que ce principe pourrait être appliqué au cas de la figure 2c). Les transferts associés sont référencés 0. sur les figures 2a-2c

Ces données peuvent indiquer pour chaque marchand (les bénéficiaires de transactions) le nombre de transaction avec eux depuis un certain laps de temps et/ou les montants associés. De façon préférée, la géolocalisation n'est pas impliquée.

La liste peut quant à elle être sommaire et simplement lister les marchands pour lesquels on considère que l'utilisateur a une utilisation « récurrente » au sens d'un critère prédéterminé, par exemple « au moins quatre dépenses dans le mois précédent pour un total d'au moins 100€ », ou peut associer à chaque marchand un seuil de paiement en procédure simplifiée comme il sera expliqué plus loin.

L'idée est que la présence d'un marchand dans la liste définisse un niveau de risque faible associé à l'utilisation d'un module de transaction du terminal 1 pour une transaction avec ce marchand, et autorise ainsi une procédure d'authentification simplifiée de l'utilisateur du moyen de paiement électronique 1, 10 (sans authentification de l'utilisateur, c'est-à-dire typiquement sans saisie de code PIN) pour des montants plus élevés qu'à l'accoutumée.

Cette étape peut être mise en œuvre régulièrement, où au début de la transaction (en particulier dans le cas où le moyen de transaction électronique 1, 10 est une carte physique ne pouvant communiquer avec le serveur 21 que via un TPE 2).

Dans une étape (b), l'élément de sécurité 12 reçoit une requête de transaction visant un module de transaction de ladite pluralité, par exemple émise depuis un TPE 2 en connexion avec le terminal 1, en particulier une fois que l'utilisateur ait signalé vouloir mettre en œuvre une transaction via une carte de

paiement dématérialisée qu'il a choisi par exemple sur son wallet. Cette étape est référencée 1. sur les figures 2a-2c.

La requête comprend au moins un montant de ladite transaction et un identifiant du bénéficiaire de ladite transaction (identifiant du marchand).

On note que le TPE 2 peut dans cette étape interroger la matrice des moyens de paiement actifs, de sorte à sélectionner (à l'aide d'un filtre) l'instance (le module de transaction) qui sera en charge de la transaction.

Dans une étape (c), est déterminé par l'élément de sécurité 12, en particulier par interrogation du module de risque, une procédure d'authentification de l'utilisateur parmi une pluralité de procédure en fonction desdits montant et identifiant du bénéficiaire de ladite transaction reçus, et de ladite liste d'identifiants de bénéficiaires de transactions récurrents. Cette étape est référencée 2. sur les figures 2a-2c.

Comme expliqué, de façon préférée ladite procédure d'authentification de l'utilisateur du moyen de paiement électronique 1, 10 est déterminée entre une procédure normale et une procédure simplifiée, mais on peut envisager plus de deux types de procédures si des authentifications supplémentaires étaient demandés pour des transactions de très haute valeur par exemple.

Comme expliqué précédemment, de façon particulièrement préférée ladite procédure normale comprend la vérification d'un code confidentiel saisi par l'utilisateur et/ou d'un paramètre biométrique de l'utilisateur, telle que son empreinte digitale (mais préférentiellement uniquement la vérification du code confidentiel), alors que la procédure simplifiée ne comprend pas de vérification d'un code confidentiel saisi par l'utilisateur (procédure « rapide » généralement sans contact). Pour reformuler encore, la procédure simplifiée ne comprend aucune authentification de l'utilisateur autre que la possession du moyen de transaction 1, 10.

Plus précisément, et contrairement à l'art antérieur où seul le seuil de régulation était pris en compte, le niveau de risque définit un seuil de montant de transaction pour passage en procédure simplifiée, i.e. le montant maximal pour lequel la saisie du code PIN de l'utilisateur (ou toute autre procédure d'authentification telle qu'une mesure biométrique) n'est pas requise pour activer le module de transaction.

De façon pratique, le choix entre procédure simplifiée et procédure normale est déterminé par comparaison du montant de la transaction avec un seuil, ce seuil

étant plus bas pour un marchand non récurrent (qui n'est pas dans la liste et dont la transaction est considérée à risque normal), pour un marchand récurrent (dans la liste et donc la transaction est considérée à risque faible).

Ainsi, dans la procédure normale un seuil dit par défaut est utilisé, correspondant avantageusement au seuil de régulation (aujourd'hui 20€), et dans la procédure simplifiée au moins un seuil spécifique supérieur au premier seuil est utilisé, par exemple 50€.

Dans l'exemple d'une dépense de 45€, le code PIN de l'utilisateur sera demandé uniquement chez des marchands non-récurrents. Plus précisément, le paiement sans contact « rapide » sera autorisé chez le marchand récurrent (car on est en dessous du deuxième seuil de 50€), alors qu'il sera refusé chez le marchand non-récurrent (car on est au-dessus du premier seuil de 20€) et il lui sera demandé se saisir son code PIN (dans le cas d'une carte physique 10, il faudra l'insérer dans le lecteur).

A noter qu'au sein de la liste, certains marchands peuvent même être considérés « très récurrents » s'ils vérifient des critères encore plus élevés de montant et de fréquence de dépense. Cela peut se traduire par des seuils encore plus élevés.

Ainsi, de façon particulièrement préférée, chaque marchand de la liste est associé à un seuil calculé par le serveur 21 ou par le module de gestion wallet (i.e. par le module traitement de données 11). Chaque seuil de ladite liste est supérieur au seuil par défaut pour que le procédé ait un intérêt.

Dans ce mode de réalisation l'étape (c) comprend alors :

- Si ledit identifiant reçu du bénéficiaire de la transaction appartient à ladite liste, la procédure d'authentification de l'utilisateur du moyen de paiement électronique 1, 10 est déterminée comme étant la procédure simplifiée si le montant de transaction reçu est inférieur ou égal au seuil associé dans la liste à l'identifiant reçu ;
- Si ledit identifiant reçu du bénéficiaire de la transaction n'appartient à ladite liste, la procédure d'authentification de l'utilisateur du moyen de paiement électronique 1, 10 est déterminée comme étant la procédure simplifiée si le montant de transaction reçu est inférieur ou égal au seuil par défaut ;
- Sinon (dans tous les autres cas), la procédure d'authentification de l'utilisateur du moyen de paiement électronique 1, 10 est déterminée comme étant la procédure normale.

On note que dans la mesure où une autorisation de procédure simplifiée à un seuil supérieur au seuil de régulation constitue une dérogation aux standards de sécurité, il est particulièrement intéressant que l'étape (c) soit gérée par un module de risque stocké dans l'élément de sécurité 12.

Un tel élément de sécurité, tel qu'une carte d'identification d'abonné est un dispositif physique de confiance quasi-impossible à infecter par un Cheval de Troie, car l'installation d'applications dans ces cartes est limitée à des entités bien identifiées, et contrôlées par l'opérateur et/ou ou l'émetteur du service en lien avec le fabricant de l'élément de sécurité 12.

La procédure d'authentification déterminée doit alors être complétée, de sorte que dans une étape (d) ledit module de transaction puisse être activé si ladite procédure d'authentification déterminée est complétée, en vue de l'émission d'une autorisation de transaction en réponse à ladite requête de transaction.

Plus précisément, l'étape (d) comprend en cas de procédure normale l'émission par le module de transaction visé, à destination du module de gestion, d'une requête de présentation d'un code confidentiel associé au module de transaction, le module de gestion étant configuré pour requérir et obtenir via l'interface 14 du terminal mobile 1 ledit code confidentiel (ou sur une interface du TPE 2 dans le cas où le moyen de transaction électronique est une carte électronique physique 10), étape notée 3. sur les figures 2a-2c.

Sur réception du code confidentiel valide (sinon il renvoie un message d'erreur, et de façon préférée se bloque au bout de trois erreurs) le wallet s'active, et il active le module de transaction visé (étape 4. des figures), de sorte que ce dernier émette in fine l'autorisation de transaction en réponse à ladite requête de transaction.

Dans un premier mode de réalisation, le module de gestion de type wallet émet le code confidentiel saisi au module de transaction visé.

Alternativement, le wallet émet d'une commande d'activation du module de transaction visé (plutôt que le code seul) en réponse, ce qui permet d'améliorer encore la sécurité d'un cran. Toute interception de requêtes et manipulation de l'élément de sécurité 12 devient impossible.

Le module de transaction activé peut alors finir la mise en œuvre de la transaction de manière classique. De façon préférée, dans le cas de paiements, le procédé comprend à ce titre en outre une étape (d) de transmission de l'autorisation de transaction à un serveur bancaire 3 associé à ladite carte

électronique (physique ou virtualisée) via le réseau 20. Typiquement, dans l'étape 5. représentée, l'autorisation de paiement est transférée au TPE 2 de sorte que ce dernier puisse rapporter auprès du serveur 3 dans une étape 6.

Apprentissage

De façon préférée, ladite liste d'identifiants de bénéficiaires de transactions récurrents évolue dynamiquement.

Pour cela, le procédé comprend avantageusement une étape subséquente (e) de notification de la transaction autorisée au serveur 21 de sorte à mettre à jour ladite liste d'identifiants de bénéficiaires de transactions récurrents (plus précisément les données d'historique représentatives de transactions précédentes). Le serveur 21 peut notifier à son tour le module wallet.

Il peut ainsi être prévu que la première transaction chez un marchand donné est toujours gérée vis-à-vis du seuil de régulation, puis si un certain nombre et/ou montant de transaction est atteint pour ce marchand il vient rejoindre la liste de sorte à y faciliter les procédures simplifiées. A noter que cela peut être soumis à l'autorisation de l'utilisateur. Il peut par exemple être notifié (via le wallet) qu'un marchand peut rejoindre la liste des marchands récurrents, et donc qu'un nouveau seuil de paiement sans authentification lui est proposé s'il l'accepte.

Le seuil associé à un marchand récurrent peut évoluer dans le temps, à la hausse ou à la baisse, en fonction de l'historique de transactions. Il peut même être prévu qu'il quitte la liste si une certaines périodes sans transactions avec lui s'écoule.

A noter que le serveur 21 peut être en contact avec les marchands, ceux-ci pouvant accepter ou non le nouveau seuil de paiement. Plus précisément, il peut être prévu que tous les marchand intéressés envoient leur identifiant à au serveur 21, et seuls ceux l'ayant fait peuvent être inclus dans la liste de marchands récurrents. Pour les autres, le seuil restera au seuil de régulation dans tous les cas.

Moyen de paiement électronique

Selon un deuxième aspect, l'invention concerne le moyen de transaction électronique 1, 10 pour la mise en œuvre du procédé selon le premier aspect

Sur ce moyen 1, 10 est stocké au moins un module de transaction adapté pour autoriser une transaction lorsqu'il est activé (en particulier sur un élément de sécurité 12), et comprenant une unité de communication 13 avec un réseau 20.

De façon préférée le moyen 1, 10 est soit une carte électronique physique 10, soit un terminal mobile 1 comprenant également un module de traitement de données 11 (un processeur). Dans le deuxième cas, le module de transaction est associé à une carte électronique « virtualisée », et adapté pour autoriser une transaction pour le compte de cette carte électronique lorsqu'il est activé. Son élément de sécurité 12 est avantageusement sous la forme d'une carte d'identification d'abonné, mais également sous la forme d'une zone du module de traitement de données 11 ou d'un composant externe éventuellement amovible, etc.

Dans tous les cas, le moyen de transaction électronique 1, 10 (et plus précisément son élément de sécurité 12 s'il s'agit d'un terminal mobile 1, bien qu'on comprendra qu'une carte électronique physique 10 constitue un élément de sécurité par définition) est configuré pour :

- Obtenir (au niveau d'un module de risque, éventuellement via un module wallet traitant des données d'historique de transaction) depuis un serveur 21 du réseau 20 via l'unité de communication 13 une liste d'identifiants de bénéficiaires de transactions récurrents ;
- recevoir une requête de transaction visant ledit module de transaction (par exemple depuis un TPE 2), la requête comprenant au moins un montant de ladite transaction et un identifiant du bénéficiaire de ladite transaction ;
- déterminer (par interrogation du module de risque) une procédure d'authentification de l'utilisateur du moyen de paiement électronique 1, 10 parmi une pluralité de procédure en fonction desdits montant et identifiant du bénéficiaire de ladite transaction reçus, et de ladite liste d'identifiants de bénéficiaires de transactions récurrents ;
- Si ladite procédure d'authentification déterminée est complétée (par sollicitation d'un saisie d'un code confidentiel si une procédure normale est demandée), activer ledit module de transaction, et émettre une autorisation de transaction en réponse à ladite requête de transaction

Produit programme d'ordinateur

Selon un troisième et un quatrième aspects, l'invention concerne un produit programme d'ordinateur comprenant des instructions de code pour l'exécution (en particulier sur l'élément de sécurité 12 du terminal 1 ou sur une carte physique 10) d'un procédé selon le premier aspect de l'invention de mise en œuvre d'une transaction depuis un moyen de transaction électronique 1, 10 d'un utilisateur, ainsi que des moyens de stockage lisibles par un équipement informatique (une mémoire de l'élément de sécurité 12) sur lequel on trouve ce produit programme d'ordinateur.

REVENDICATIONS

1. Procédé de mise en œuvre d'une transaction depuis un moyen de transaction électronique (1, 10) d'un utilisateur, sur lequel est stocké au moins un module de transaction adapté pour autoriser une transaction lorsqu'il est activé, le moyen de transaction électronique (1, 10) comprenant en outre une unité de communication (13) avec un réseau (20) ;

Le procédé étant caractérisé en ce qu'il comprend la mise en œuvre par le moyen de paiement électronique (1, 10) d'étapes de :

(a) Obtention depuis un serveur (21) du réseau (20) via l'unité de communication (13) d'une liste d'identifiants de bénéficiaires de transactions récurrents ;

(b) Obtention d'au moins un seuil de bénéficiaire associé à au moins un identifiant de bénéficiaire de transaction récurrent de ladite liste

(c) réception d'une requête de transaction visant ledit module de transaction, la requête comprenant au moins un montant de ladite transaction et un identifiant du bénéficiaire de ladite transaction ;

(d) Détermination d'une procédure d'authentification de l'utilisateur du moyen de paiement électronique (1, 10) parmi une pluralité de procédure en fonction desdits montant et identifiant du bénéficiaire de ladite transaction reçus, et de ladite liste d'identifiants de bénéficiaires de transactions récurrents, ladite pluralité de procédures comprenant au moins :

a. une procédure normale comprenant la vérification d'un paramètre d'authentification de l'utilisateur ;

b. une procédure simplifiée ne comprenant pas de vérification d'un paramètre d'authentification de l'utilisateur.

(e) Si ledit identifiant reçu du bénéficiaire de la transaction appartient à ladite liste, la procédure d'authentification de l'utilisateur du moyen de paiement électronique (1, 10) est déterminée comme étant la procédure simplifiée si le montant de transaction reçu est inférieur ou égal à un seuil de bénéficiaire associé dans la liste à l'identifiant reçu.

(f) Si ladite procédure d'authentification déterminée est complétée, activation dudit module de transaction, et émission d'une autorisation de transaction en réponse à ladite requête de transaction.

2. Procédé selon la revendication 1, dans lequel la vérification d'un paramètre d'authentification de l'utilisateur comprend la vérification d'un code confidentiel saisi par l'utilisateur et/ou la vérification d'un paramètre biométrique de l'utilisateur,

3. Procédé selon la revendication 1, dans lequel un seuil [du bénéficiaire] est obtenu en fonction d'au moins une donnée parmi :

- le nombre de transactions effectuées avec ledit bénéficiaire de transactions ;
- le montant associé aux transactions effectuées avec ledit bénéficiaire de transactions

4. Procédé selon la revendication 1, dans lequel le moyen de transaction électronique est choisi parmi une carte électronique physique (10) et un terminal mobile (1) sur lequel ledit module de transaction est associé à une carte électronique, et adapté pour autoriser une transaction pour le compte de ladite carte électronique lorsqu'il est activé.

5. Procédé selon la revendication 4, dans lequel le moyen de transaction électronique est un terminal mobile (1) comprenant un module de traitement de données (11) et un élément de sécurité (12) sur lequel est stocké ledit module de transaction.

6. Procédé selon la revendication 5, dans lequel l'élément de sécurité (12) est soit un élément matériel choisi parmi une carte d'identification d'abonné et un espace d'exécution sécurisé du module de traitement de données (11) du terminal (1), soit un élément logiciel émulé par le module de traitement de données (11) du terminal (1) conformément à l'architecture Emulation de Cartes Hebergées, HCE.

7. Procédé selon l'une des revendications 5 et 6, dans lequel l'élément de sécurité (12) met en œuvre ledit module de transaction et un module de risque stockant ladite liste d'identifiants de bénéficiaires de transactions récurrents, et le module de traitement de données (11) met en œuvre un module de gestion du ou des modules de transaction, l'étape (b) comprenant l'interrogation du module de risque par le module de transaction visé.

8. Procédé selon la revendication 7, dans lequel l'étape (a) comprend la réception par le module de gestion de données d'historique représentatives de transactions précédentes, la génération de ladite liste d'identifiants de bénéficiaires de transactions récurrents par le module de gestion à partir desdites données d'historique représentatives de transactions précédentes, et la transmission de ladite liste au module de risque.

9. Procédé selon l'une des revendications 1 à 8, dans lequel le moyen de transaction électronique (1, 10) est un moyen de paiement électronique, la requête de transaction étant reçue à l'étape (a) depuis un terminal de paiement électronique (2) en communication sans fil avec le moyen de paiement électronique (1, 10), l'autorisation de transaction étant émise à l'étape (d) à destination du terminal de paiement électronique (2).

10. Procédé selon la revendication 7, comprenant en outre une étape (e) de transmission de l'autorisation de transaction à un serveur bancaire (3) associé à une carte bancaire via le réseau (20).

11. Procédé selon la revendication 10 en combinaison avec l'une des revendications 7 et 8, dans lequel l'étape (d) comprend en cas de procédure normale l'émission par le module de transaction visé, à destination du module de gestion, d'une requête de présentation d'un code confidentiel associé au module de transaction, le module de gestion étant configuré pour requérir et obtenir via une interface (14) du terminal ledit code confidentiel.

12. Procédé selon la revendication 1, dans lequel un seuil par défaut est stocké dans le moyen de transaction électronique (1, 10), chaque seuil de ladite liste étant supérieur au seuil par défaut, l'étape (c) comprenant :

- Si ledit identifiant reçu du bénéficiaire de la transaction n'appartient à ladite liste, la procédure d'authentification de l'utilisateur du moyen de paiement électronique (1, 10) est déterminée comme étant la procédure simplifiée si le montant de transaction reçu est inférieur ou égal au seuil par défaut.

13. Procédé selon l'une des revendications 1 à 12, comprenant une étape (e) de notification de la transaction autorisée au serveur (21) de sorte à mettre à jour ladite liste d'identifiants de bénéficiaires de transactions récurrents.

14. Moyen de transaction électronique (1, 10) sur lequel est stocké au moins un module de transaction adapté pour autoriser une transaction lorsqu'il est activé, et comprenant une unité de communication (13) avec un réseau (20),

Le moyen de transaction électronique (1, 10) étant configuré pour :

- Obtenir depuis un serveur (21) du réseau (20) via l'unité de communication (13) une liste d'identifiants de bénéficiaires de transactions récurrents ;
- Obtenir au moins un seuil de bénéficiaire associé à au moins un identifiant de bénéficiaire de transaction récurrent de ladite liste ;
- recevoir une requête de transaction visant ledit module de transaction, la requête comprenant au moins un montant de ladite transaction et un identifiant du bénéficiaire de ladite transaction ;
- déterminer une procédure d'authentification de l'utilisateur du moyen de paiement électronique (1, 10) parmi une pluralité de procédure en fonction desdits montant et identifiant du bénéficiaire de ladite transaction reçus, et de ladite liste d'identifiants de bénéficiaires de transactions récurrents ; ladite pluralité de procédures comprenant au moins :
  a. une procédure normale comprenant la vérification d'un paramètre d'authentification de l'utilisateur ;
  b. une procédure simplifiée ne comprenant pas de vérification d'un paramètre d'authentification de l'utilisateur ;
- Si ledit identifiant reçu du bénéficiaire de la transaction appartient à ladite liste, déterminer la procédure d'authentification de l'utilisateur du moyen de paiement électronique (1, 10) comme étant la procédure simplifiée si le montant de transaction reçu est inférieur ou égal à un seuil de bénéficiaire associé dans la liste à l'identifiant reçu ;
- Si ladite procédure d'authentification déterminée est complétée, activer ledit module de transaction, et émettre une autorisation de transaction en réponse à ladite requête de transaction

15. Moyen de transaction électronique (1, 10) selon la revendication 14, étant un terminal mobile (1), le module de transaction étant associé à une carte électronique, et adapté pour autoriser une transaction pour le compte de ladite carte électronique lorsqu'il est activé.

16. Produit programme d'ordinateur comprenant des instructions de code pour l'exécution d'un procédé selon l'une des revendications 1 à 13 de mise en œuvre d'une transaction depuis un moyen de transaction électronique (1, 10) d'un utilisateur, lorsque ledit programme est exécuté par un ordinateur.

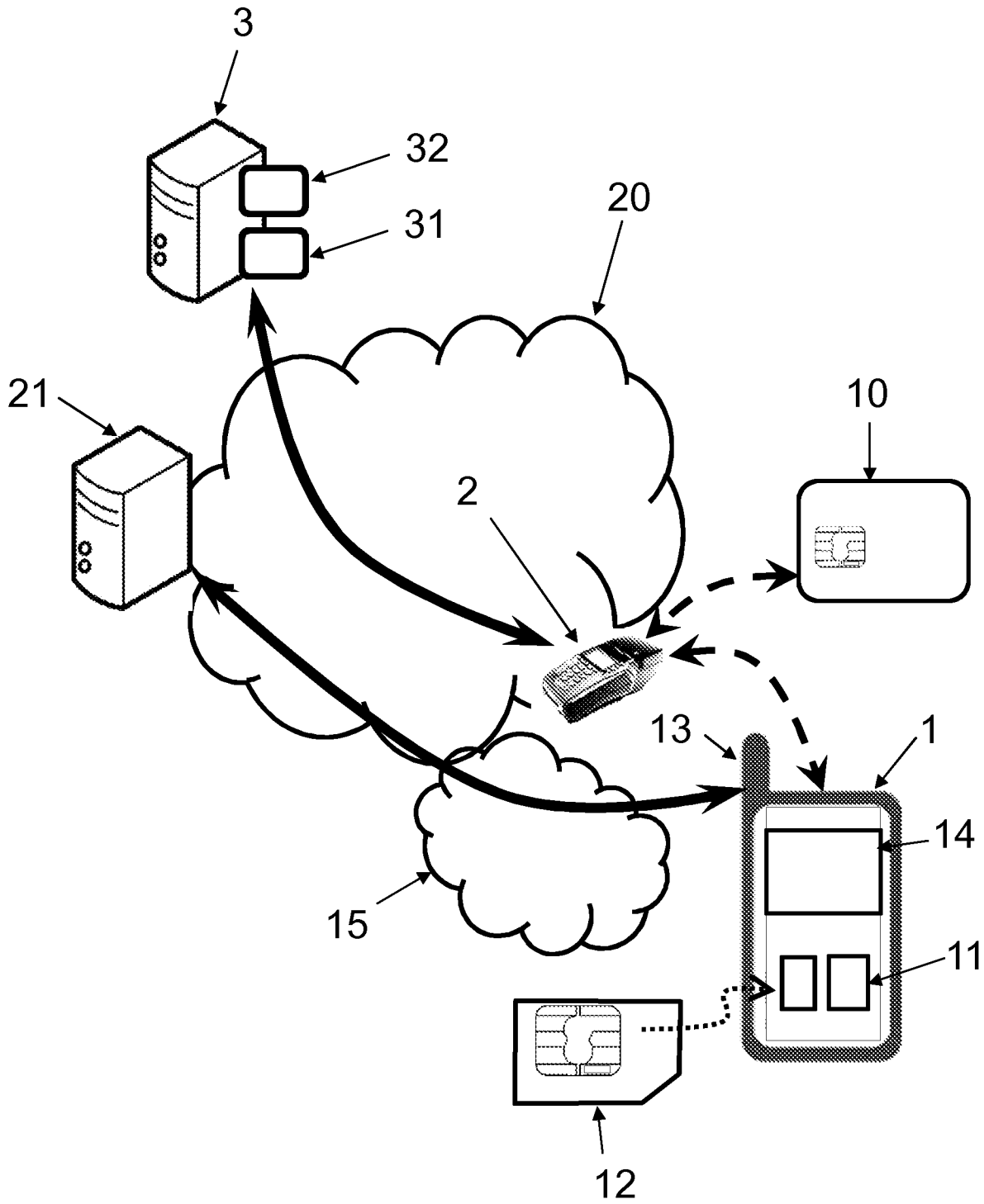

FIG. 1

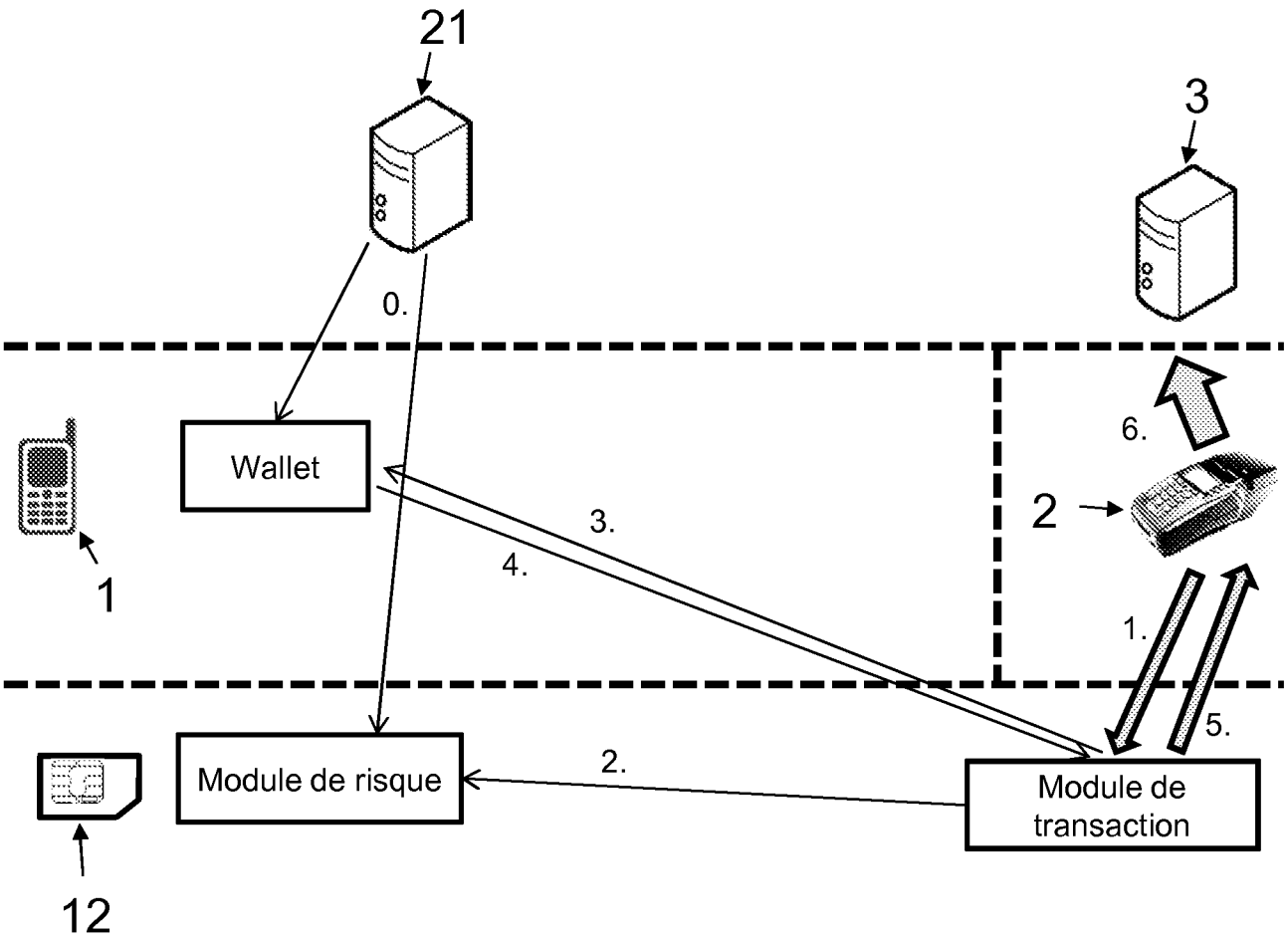
21
3
0.
Wallet
1
3.
4.
6.
2
1.
5.
Module de risque
2.
Module de transaction
12

FIG. 2a

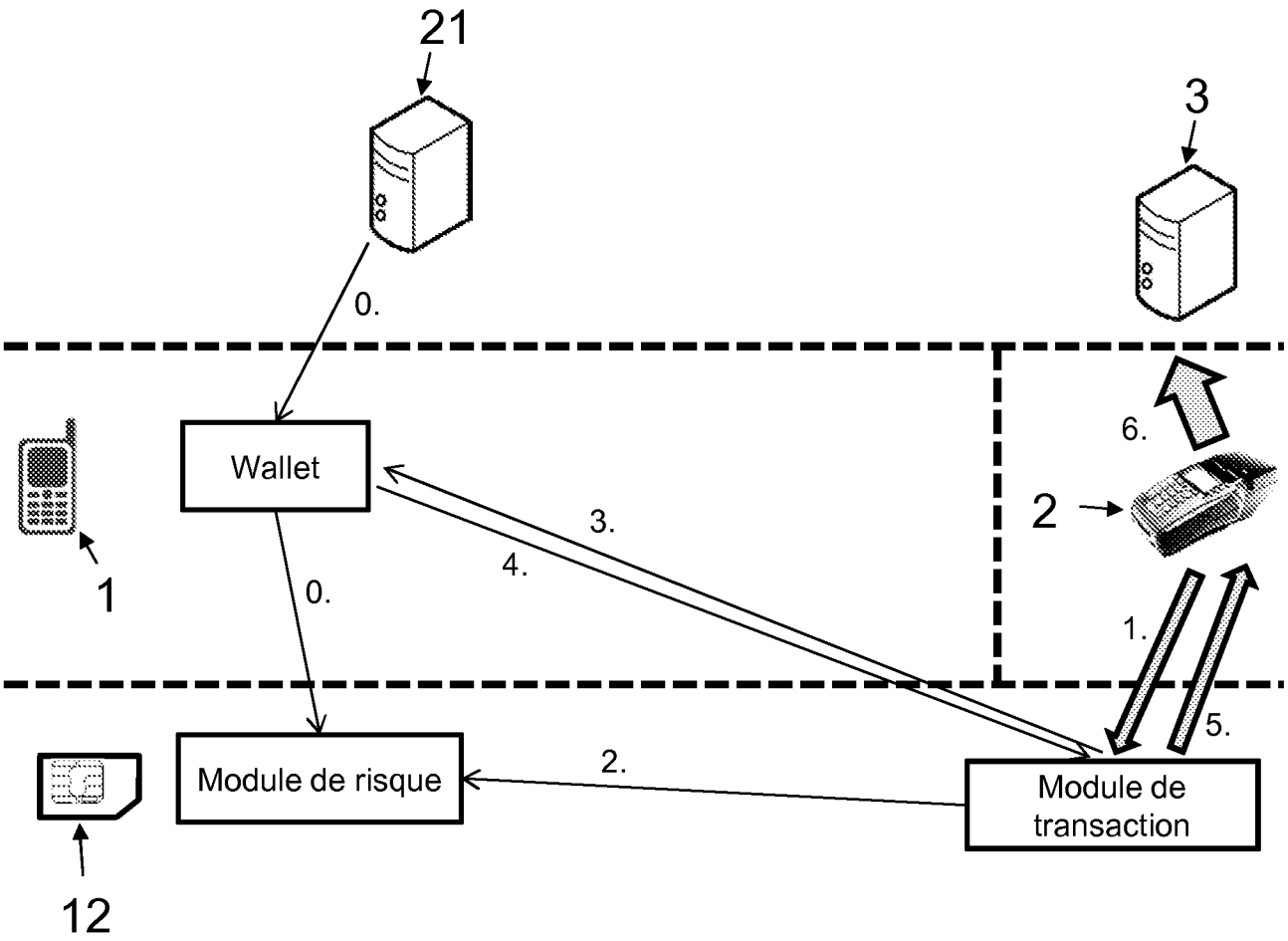
21
3
0.
Wallet
6.
2
3.
4.
1
0.
1.
5.
Module de risque
2.
Module de transaction
12

FIG. 2b

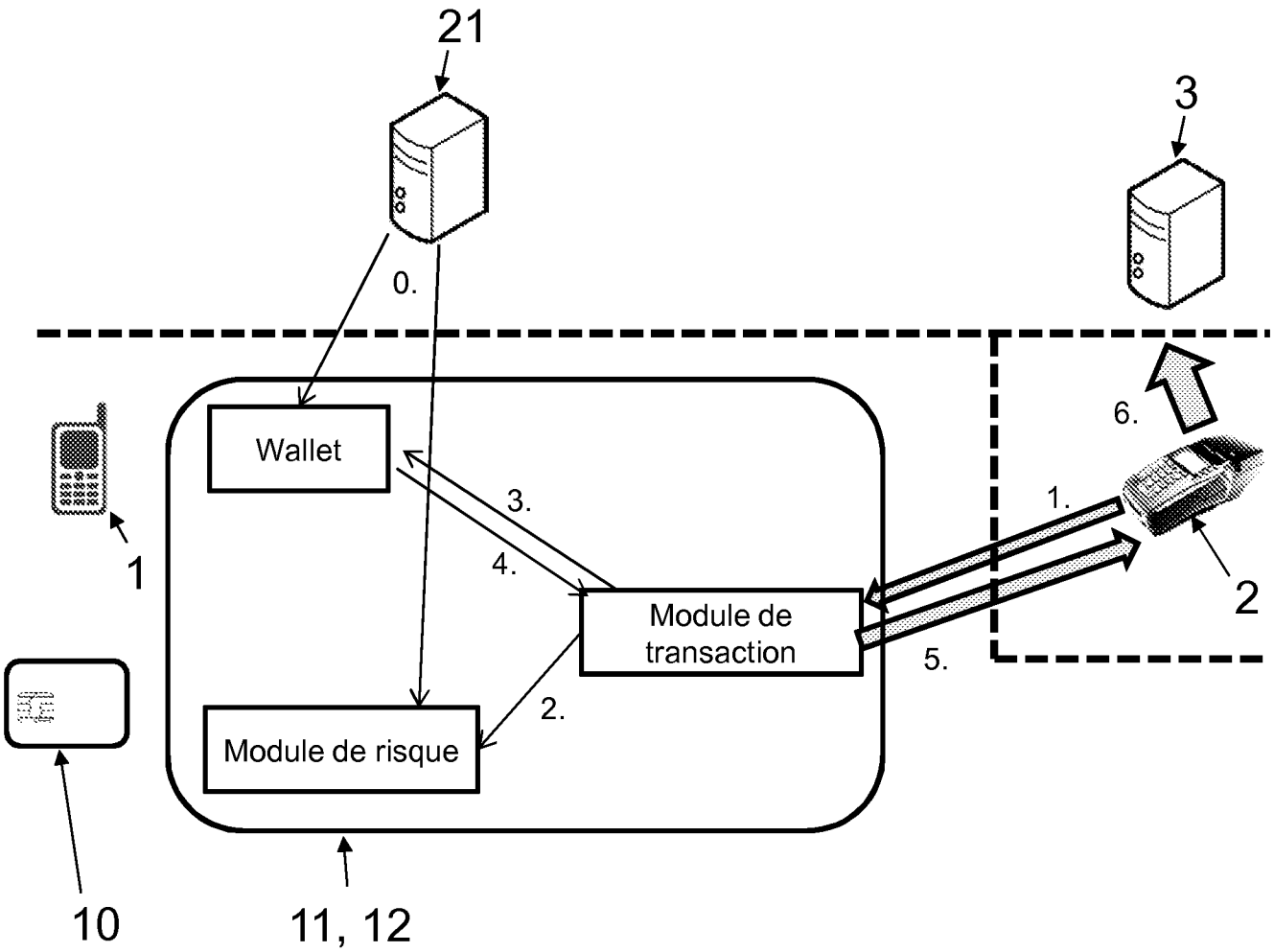
21
3
0.
Wallet
3.
4.
Module de transaction
Module de risque
2.
1.
5.
6.
1
2
10
11, 12

FIG. 2c

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2017/052156

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q20/02 G06Q20/20 G06Q20/32 G06Q20/34 G06Q20/36 G06Q20/40
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 2016/132880 A1 (O'REGAN ALAN JOSEPH [ZA] ET AL) 12 May 2016 (2016-05-12) abstract; figures paragraphs [0064] - [0083], [0088] - [0108]	1-16
X	EP 2 261 849 A1 (ALCATEL LUCENT [FR]) 15 December 2010 (2010-12-15) abstract; figures paragraphs [0005], [0023] - [0045]	1-16
X	US 8 690 054 B1 (CUMMINS MICHAEL D [CA] ET AL) 8 April 2014 (2014-04-08) abstract; figures column 2, line 15 - column 4, line 18 column 5, line 1 - column 6, line 27	1-16

-/--

[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
3 October 2017	12/10/2017

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	Breugelmans, Jan

1

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2017/052156

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 8 135 624 B1 (RAMALINGAM HARSHA [US] ET AL) 13 March 2012 (2012-03-13) abstract; figures	1-16
A	US 2011/320345 A1 (TAVEAU SEBASTIEN [US] ET AL) 29 December 2011 (2011-12-29) abstract; figures	1-16
A	US 2016/086166 A1 (POMEROY JEFF [US] ET AL) 24 March 2016 (2016-03-24) abstract; figures	1-16
A	US 2005/216424 A1 (GANDRE THOMAS R [US] ET AL) 29 September 2005 (2005-09-29) abstract; figures	1-16

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2017/052156

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2016132880 A1	12-05-2016	AU 2014285774 A1	07-01-2016
		CN 105518732 A	20-04-2016
		EP 3017413 A1	11-05-2016
		HK 1217804 A1	20-01-2017
		KR 20160015375 A	12-02-2016
		US 2016132880 A1	12-05-2016
		WO 2015001473 A1	08-01-2015
EP 2261849 A1	15-12-2010	EP 2261849 A1	15-12-2010
		FR 2946776 A1	17-12-2010
US 8690054 B1	08-04-2014	CA 2846305 A1	29-11-2014
		US 8690054 B1	08-04-2014
		US 8864024 B1	21-10-2014
US 8135624 B1	13-03-2012	US 8135624 B1	13-03-2012
		US 8255284 B1	28-08-2012
		US 8341029 B1	25-12-2012
		US 8521131 B1	27-08-2013
		US 9107064 B1	11-08-2015
		US 9386507 B1	05-07-2016
		US 9609577 B1	28-03-2017
		US 9697508 B1	04-07-2017
		US 9723131 B1	01-08-2017
		US 9760885 B1	12-09-2017
		US 9767474 B1	19-09-2017
		US 2011238474 A1	29-09-2011
		US 2011238514 A1	29-09-2011
		US 2011238517 A1	29-09-2011
		US 2017163655 A1	08-06-2017
US 2011320345 A1	29-12-2011	AU 2011276661 A1	31-01-2013
		BR 112012033740 A2	22-11-2016
		CA 2805026 A1	12-01-2012
		CN 103080960 A	01-05-2013
		EP 2589003 A1	08-05-2013
		KR 20130086205 A	31-07-2013
		RU 2013103698 A	10-08-2014
		US 2011320345 A1	29-12-2011
		US 2017206519 A1	20-07-2017
		WO 2012005954 A1	12-01-2012
US 2016086166 A1	24-03-2016	NONE	
US 2005216424 A1	29-09-2005	AU 2005227891 A1	13-10-2005
		CA 2560854 A1	13-10-2005
		CN 101124596 A	13-02-2008
		EP 1730689 A2	13-12-2006
		US 2005216424 A1	29-09-2005
		WO 2005094442 A2	13-10-2005

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2017/052156

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06Q20/02 G06Q20/20 G06Q20/32 G06Q20/34 G06Q20/36
G06Q20/40
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 2016/132880 A1 (O'REGAN ALAN JOSEPH [ZA] ET AL) 12 mai 2016 (2016-05-12) abrégé; figures alinéas [0064] - [0083], [0088] - [0108] -----	1-16
X	EP 2 261 849 A1 (ALCATEL LUCENT [FR]) 15 décembre 2010 (2010-12-15) abrégé; figures alinéas [0005], [0023] - [0045] -----	1-16
X	US 8 690 054 B1 (CUMMINS MICHAEL D [CA] ET AL) 8 avril 2014 (2014-04-08) abrégé; figures colonne 2, ligne 15 - colonne 4, ligne 18 colonne 5, ligne 1 - colonne 6, ligne 27 ----- -/--	1-16

[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
3 octobre 2017	12/10/2017

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	Breugelmans, Jan

1

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 8 135 624 B1 (RAMALINGAM HARSHA [US] ET AL) 13 mars 2012 (2012-03-13) abrégé; figures	1-16
A	US 2011/320345 A1 (TAVEAU SEBASTIEN [US] ET AL) 29 décembre 2011 (2011-12-29) abrégé; figures	1-16
A	US 2016/086166 A1 (POMEROY JEFF [US] ET AL) 24 mars 2016 (2016-03-24) abrégé; figures	1-16
A	US 2005/216424 A1 (GANDRE THOMAS R [US] ET AL) 29 septembre 2005 (2005-09-29) abrégé; figures	1-16

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2017/052156

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2016132880 A1	12-05-2016	AU 2014285774 A1	07-01-2016
		CN 105518732 A	20-04-2016
		EP 3017413 A1	11-05-2016
		HK 1217804 A1	20-01-2017
		KR 20160015375 A	12-02-2016
		US 2016132880 A1	12-05-2016
		WO 2015001473 A1	08-01-2015
EP 2261849 A1	15-12-2010	EP 2261849 A1	15-12-2010
		FR 2946776 A1	17-12-2010
US 8690054 B1	08-04-2014	CA 2846305 A1	29-11-2014
		US 8690054 B1	08-04-2014
		US 8864024 B1	21-10-2014
US 8135624 B1	13-03-2012	US 8135624 B1	13-03-2012
		US 8255284 B1	28-08-2012
		US 8341029 B1	25-12-2012
		US 8521131 B1	27-08-2013
		US 9107064 B1	11-08-2015
		US 9386507 B1	05-07-2016
		US 9609577 B1	28-03-2017
		US 9697508 B1	04-07-2017
		US 9723131 B1	01-08-2017
		US 9760885 B1	12-09-2017
		US 9767474 B1	19-09-2017
		US 2011238474 A1	29-09-2011
		US 2011238514 A1	29-09-2011
		US 2011238517 A1	29-09-2011
		US 2017163655 A1	08-06-2017
US 2011320345 A1	29-12-2011	AU 2011276661 A1	31-01-2013
		BR 112012033740 A2	22-11-2016
		CA 2805026 A1	12-01-2012
		CN 103080960 A	01-05-2013
		EP 2589003 A1	08-05-2013
		KR 20130086205 A	31-07-2013
		RU 2013103698 A	10-08-2014
		US 2011320345 A1	29-12-2011
		US 2017206519 A1	20-07-2017
		WO 2012005954 A1	12-01-2012
US 2016086166 A1	24-03-2016	AUCUN	
US 2005216424 A1	29-09-2005	AU 2005227891 A1	13-10-2005
		CA 2560854 A1	13-10-2005
		CN 101124596 A	13-02-2008
		EP 1730689 A2	13-12-2006
		US 2005216424 A1	29-09-2005
		WO 2005094442 A2	13-10-2005