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

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
14 juillet 2016 (14.07.2016)

WIPO | PCT

(10) Numéro de publication internationale
WO 2016/110590 A1

(51) Classification internationale des brevets :
G06Q 20/34 (2012.01) *G06Q 20/32* (2012.01)
G06Q 20/42 (2012.01) *H04W 12/08* (2009.01)
H04L 29/06 (2006.01) *G06F 21/53* (2013.01)

(21) Numéro de la demande internationale :
PCT/EP2016/050318

(22) Date de dépôt international :
8 janvier 2016 (08.01.2016)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :

1550192	9 janvier 2015 (09.01.2015)	FR
1550191	9 janvier 2015 (09.01.2015)	FR
1550193	9 janvier 2015 (09.01.2015)	FR
1551241	13 février 2015 (13.02.2015)	FR

(71) Déposant : **INGENICO GROUP** [FR/FR]; 28/32 Boulevard de Grenelle, 75015 Paris (FR).

(72) Inventeur : **QUENTIN, Pierre**; 26 rue Paul Delinge, 95880 Enghien-les-Bains (FR).

(74) Mandataire : **VIDON BREVETS & STRATÉGIE**; 90333 B, Technopôle Atalante, 16B rue de Jouanet, 35703 Rennes Cedex 7 (FR).

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

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,

[Suite sur la page suivante]

(54) **Title** : METHOD FOR PROCESSING A TRANSACTION FROM A COMMUNICATION TERMINAL

(54) **Titre** : PROCÉDÉ DE TRAITEMENT D'UNE TRANSACTION À PARTIR D'UN TERMINAL DE COMMUNICATION

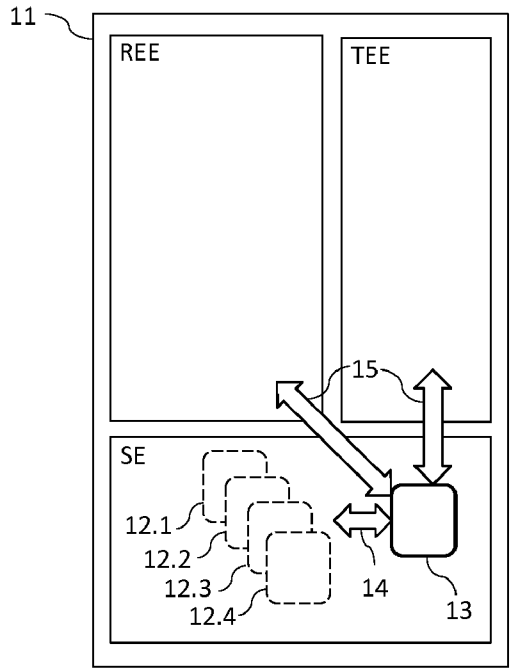

Fig. 1

(57) **Abstract** : The invention relates to a security module (SE) built into a mobile communication terminal (11). Such a module includes: at least one first transaction-processing application (12) including at least one interface for securely communicating with a communication network, and at least one second application (13) for processing secure data including at least one interface for communicating with an execution environment of said communication terminal, said first application being capable of requesting at least one data item from said second application.

(57) **Abrégé** : L'invention se rapporte à module de sécurisation (SE) intégré au sein d'un terminal de communication mobile (11). Un tel module comprend : au moins une première application (12) de traitement de transaction comprenant au moins une interface de communication avec un réseau de communication de manière sécurisée, et au moins une deuxième application (13) de traitement de données sécurisées comprenant au moins une interface de communication avec un environnement d'exécution dudit terminal de communication, ladite première application étant en mesure de requérir au moins une donnée auprès de ladite deuxième application.

WO 2016/110590 A1

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))*

Procédé de traitement d'une transaction à partir d'un terminal de communication.

1. Domaine

La technique proposée se rapporte au traitement de transactions en ligne, et plus particulièrement au traitement de transactions à partir d'un terminal de communication, sous une forme sécurisée.

2. Art Antérieur

Deux modes de transactions coexistent lorsqu'un utilisateur souhaite effectuer une transaction de paiement à partir d'une carte bancaire :

- le mode « carte présente » : la carte bancaire est physiquement utilisée. Elle est par exemple insérée dans un terminal de paiement, et les informations qu'elle contient sont lues directement à partir de la puce ou de la bande magnétique intégrées à la carte. Alternativement, la carte bancaire est approchée d'un terminal de paiement, et les informations sont transmises via une technologie sans contact de type NFC (de l'anglais « Near Field Communication ») ;
- le mode « carte non présente » : la carte bancaire n'est pas utilisée physiquement, mais l'utilisateur saisit les informations présentes sur cette carte (numéro de carte, cryptogramme visuel, date d'expiration, nom du porteur) pour effectuer une transaction. C'est la solution aujourd'hui majoritairement utilisée pour le paiement en ligne sur Internet par exemple.

De nombreux fabricants de terminaux de communication mobiles (typiquement des smartphones ou des tablettes) cherchent aujourd'hui développer des solutions de paiement directement intégrées au terminal mobile, permettant à l'utilisateur de s'affranchir d'avoir à se munir de sa carte bancaire lorsqu'il souhaite effectuer une transaction.

Les solutions proposées actuellement à cette fin reposent essentiellement sur une mise en œuvre basée sur le mode de transaction de type « carte non présente » décrit précédemment : dans une première phase d'initialisation du service, l'utilisateur est invité à saisir, au sein d'une application dédiée installée sur son terminal de communication, les informations associées à sa ou ses cartes bancaires (par exemple le

type de carte, le numéro de carte, le cryptogramme visuel, la date d'expiration, etc.). Ces informations sont alors enregistrées au sein même du terminal de communication. Cette phase d'initialisation terminée, l'utilisateur a alors la possibilité d'utiliser l'application dédiée pour effectuer certains paiements sans avoir à se munir de sa carte bancaire et devoir ressaisir manuellement les informations qui y sont indiquées : ces informations sont alors directement transmises par le terminal de communication au serveur de paiement.

Cette solution est néanmoins limitée. D'une part, les possibilités de transactions accessibles depuis un terminal de communication mobile sont limitées et ne concernent que les transactions en ligne reposant sur un mode « carte non présente », et la solution proposée vise alors essentiellement à éviter à l'utilisateur d'avoir à saisir lui-même les données associées à sa carte bancaire à chaque fois qu'il souhaite effectuer un paiement depuis un terminal de communication (saisie souvent fastidieuse). D'autre part cette solution soulève des problèmes de sécurité : toutes les données utiles pour réaliser une transaction étant stockées au sein même du terminal de communication, un utilisateur qui a égaré ou s'est fait subtiliser son dispositif mobile (son téléphone portable par exemple) n'est pas à l'abri qu'une personne malveillante qui a récupéré son bien accède à ces informations sensibles et réalise des transactions financières en son nom (si le terminal de communication ou l'application qui les contient sont insuffisamment sécurisés par exemple).

Ce problème de sécurisation qui se pose pour la réalisation de transactions de paiement à partir d'un terminal de communication est également rencontré dans la réalisation de transactions d'autres types : dès lors qu'une autorisation est requise pour la réalisation d'une transaction à partir d'un terminal de communication, il est risqué de stocker au sein de ce même terminal de communication les informations susceptibles de donner accès à une telle autorisation.

Il existe donc un besoin d'une solution permettant d'intégrer au sein d'un terminal de communication des moyens d'obtention d'une autorisation pour la réalisation de transactions, et qui ne présente pas au moins certains de ces problèmes de l'art antérieur.

3. Résumé

La technique proposée ne comprend pas ces inconvénients de l'art antérieur. Plus particulièrement, la technique proposée se rapporte à un Module de sécurisation (SE) intégré au sein d'un terminal de communication mobile.

Un tel module comprend :

au moins une première application de traitement de transaction comprenant au moins une interface de communication avec un réseau de communication de manière sécurisée, et

au moins une deuxième application de traitement de données sécurisées comprenant au moins une interface de communication avec un environnement d'exécution dudit terminal de communication,

ladite première application étant en mesure de requérir au moins une donnée auprès de ladite deuxième application.

Ainsi, un tel module permet à un terminal de communication d'offrir à la fois une fonctionnalité de traitement de transactions et des fonctionnalités « étendues » en adéquation avec les capacités de traitement de données du terminal de paiement. Par ailleurs, un tel module permet d'éviter une certification pour chaque typer de terminal au sein duquel il pourrait être inséré.

Selon une caractéristique particulière, ladite deuxième application comprend au moins un espace de stockage sécurisé.

Ainsi, la deuxième application est à même de gérer seule le stockage des données.

Selon une caractéristique particulière, ladite deuxième application comprend au moins une liste d'identifiants d'applications autorisées à accéder à ladite au moins une donnée.

Ainsi, l'application peut autoriser ou refuser l'accès aux données de manière contrôlée. De manière complémentaire, cette liste peut être prédéfinie et non modifiable afin de limiter les accès.

Selon une caractéristique particulière, ladite deuxième application comprend au moins une liste d'identifiants d'applications autorisées à requérir la mémorisation de

données au sein dudit espace de stockage sécurisé.

Selon une caractéristique particulière, ladite au moins une donnée appartient au groupe comprenant :

- une donnée représentative d'une carte de paiement ;
- une donnée représentative d'une association entre un identifiant de marchand d'une part, et un identifiant d'un utilisateur auprès dudit marchand d'autre part ;
- une donnée d'identification ou d'authentification biométrique.

Dans un autre mode de réalisation, il est également proposé un procédé de communication entre une première application de traitement de transactions et une deuxième application de traitement de données sécurisées, lesdites applications étant exécutées au sein d'un module de sécurisation d'un terminal de communication.

Un tel procédé comprend :

- une étape de réception, par ladite première application, d'une requête en provenance d'un réseau de communication ;
- une étape de transmission, par ladite première application, d'une requête d'obtention d'une donnée sécurisée, à destination de ladite deuxième application ;
- une étape d'obtention, par ladite deuxième application, de ladite donnée requise par la première application ;
- une étape de transmission, par ladite deuxième application, de ladite donnée requise, à destination de ladite première application ;
- une étape de transmission, par ladite première application, de ladite donnée requise à destination dudit réseau de communication.

Selon une caractéristique particulière,, préalablement à ladite étape d'obtention, par ladite deuxième application, de ladite donnée requise par la première application, une étape de vérification, par ladite deuxième application, que ladite première application est bien autorisée à accéder à ladite donnée requise.

Selon une caractéristique particulière, ladite étape d'obtention, par ladite deuxième application, de ladite donnée requise par la première application, comprend

les sous-étapes suivantes :

- transmission d'une requête d'obtention de ladite donnée à destination d'un environnement d'exécution dudit terminal de communication ;
- réception de ladite donnée requise par la première application, en provenance dudit environnement d'exécution dudit terminal de communication.

Selon une implémentation préférée, les différentes étapes des procédés selon la technique proposée sont mises en œuvre par un ou plusieurs logiciels ou programmes d'ordinateur, comprenant des instructions logicielles destinées à être exécutées par un processeur de données d'un module relais selon la technique proposée et étant conçu pour commander l'exécution des différentes étapes des procédés.

En conséquence, la technique proposée vise aussi un programme, susceptible d'être exécuté par un ordinateur ou par un processeur de données, ce programme comportant des instructions pour commander l'exécution des étapes d'un procédé tel que mentionné ci-dessus.

Ce programme peut utiliser n'importe quel langage de programmation, et être sous la forme de code source, code objet, ou de code intermédiaire entre code source et code objet, tel que dans une forme partiellement compilée, ou dans n'importe quelle autre forme souhaitable.

La technique proposée vise aussi un support d'informations lisible par un processeur de données, et comportant des instructions d'un programme tel que mentionné ci-dessus.

Le support d'informations peut être n'importe quelle entité ou dispositif capable de stocker le programme. Par exemple, le support peut comporter un moyen de stockage, tel qu'une ROM, par exemple un CD ROM ou une ROM de circuit microélectronique, ou encore un moyen d'enregistrement magnétique, par exemple une disquette (floppy disc) ou un disque dur.

D'autre part, le support d'informations peut être un support transmissible tel qu'un signal électrique ou optique, qui peut être acheminé via un câble électrique ou optique, par radio ou par d'autres moyens. Le programme selon la technique proposée peut être en particulier téléchargé sur un réseau de type Internet.

Alternativement, le support d'informations peut être un circuit intégré dans lequel le programme est incorporé, le circuit étant adapté pour exécuter ou pour être utilisé dans l'exécution du procédé en question.

Selon un mode de réalisation, la technique proposée est mise en œuvre au moyen de composants logiciels et/ou matériels. Dans cette optique, le terme "module" peut correspondre dans ce document aussi bien à un composant logiciel, qu'à un composant matériel ou à un ensemble de composants matériels et logiciels.

Un composant logiciel correspond à un ou plusieurs programmes d'ordinateur, un ou plusieurs sous-programmes d'un programme, ou de manière plus générale à tout élément d'un programme ou d'un logiciel apte à mettre en œuvre une fonction ou un ensemble de fonctions, selon ce qui est décrit ci-dessous pour le module concerné. Un tel composant logiciel est exécuté par un processeur de données d'une entité physique (terminal, serveur, passerelle, routeur, etc.) et est susceptible d'accéder aux ressources matérielles de cette entité physique (mémoires, supports d'enregistrement, bus de communication, cartes électroniques d'entrées/sorties, interfaces utilisateur, etc.).

De la même manière, un composant matériel correspond à tout élément d'un ensemble matériel (ou hardware) apte à mettre en œuvre une fonction ou un ensemble de fonctions, selon ce qui est décrit ci-dessous pour le module concerné. Il peut s'agir d'un composant matériel programmable ou avec processeur intégré pour l'exécution de logiciel, par exemple un circuit intégré, une carte à puce, une carte à mémoire, une carte électronique pour l'exécution d'un micrologiciel (firmware), etc.

Chaque composante du système précédemment décrit met bien entendu en œuvre ses propres modules logiciels.

Les différents modes de réalisation mentionnés ci-dessus sont combinables entre eux pour la mise en œuvre de la technique proposée.

4. Figures

D'autres caractéristiques et avantages de la technique proposée apparaîtront plus clairement à la lecture de la description suivante d'un mode de réalisation préférentiel, donné à titre de simple exemple illustratif et non limitatif, et des dessins annexés, parmi lesquels :

- la figure 1 décrit une architecture simplifiée d'un terminal de communication apte à être utilisé dans le cadre de la mise en œuvre de la technique proposée, selon un mode de réalisation particulier ;
- la figure 2 illustre les étapes réalisées pour la mise en œuvre d'un procédé de communication entre une première application de traitement de transactions et une deuxième application de traitement de données sécurisées, dans un mode de réalisation particulier ;
- la figure 3 décrit une architecture simplifiée d'un module de sécurisation selon un mode de réalisation particulier de la technique proposée.

5. Description

5.1 Principe général

La technique proposée ne présente pas au moins certains de ces problèmes de l'art antérieur. En effet, il est proposé ici un procédé de traitement d'une transaction effectuée en ligne, qui repose sur l'utilisation d'un terminal de communication pour l'obtention d'une autorisation de réalisation de ladite transaction. Ce terminal de communication dispose de moyens matériels et logiciels permettant d'assurer une sécurisation accrue de la transaction. Il comprend en particulier un module de sécurisation, au sein duquel est exécutée une première application, en charge de traiter la transaction côté terminal. Selon la technique proposée, une deuxième application est également exécutée au sein de ce module de sécurisation. Le rôle de cette deuxième application est d'épauler la première application, en lui fournissant, à sa demande, des données nécessaires pour poursuivre ou enrichir la transaction en cours de traitement.

Dans la technique proposée, les mêmes mécanismes d'authentification que ceux mis en œuvre dans le cadre de la réalisation d'une transaction de paiement à partir d'une carte bancaire dans un mode « carte présente » sont mis en œuvre au sein du terminal de communication, dans le but d'obtenir une autorisation pour la réalisation d'une transaction à partir dudit terminal de communication. Un terminal de communication ne présente cependant pas les mêmes limitations qu'une carte à puce en termes de ressources (et notamment en termes de mémoire). Aussi, l'utilisation d'un terminal de communication permet de tirer avantageusement parti des ressources

propres d'un tel dispositif pour contribuer à la mise en œuvre de la transaction. En particulier, le principe général de la technique proposée consiste à fournir à l'application de traitement de la transaction mis en œuvre au niveau du terminal de communication – qui est une application similaire à celle exécutée au sein d'une carte de paiement – des moyens permettant d'obtenir des informations complémentaires disponibles au sein du terminal de communication. Ces moyens prennent la forme d'une deuxième application, apte à communiquer avec ladite première application de traitement, pour lui fournir ces informations complémentaires, qui peuvent être ou bien des données nécessaires à la poursuite de la transaction (par exemple des données biométriques permettant de garantir une sécurisation accrue de la transaction), ou bien des données utiles pour la mise en œuvre de services complémentaires en lien avec la présente transaction (créditer des points de fidélité par exemple).

On présente, en relation avec la **figure 1**, une architecture simplifiée d'un terminal de communication (11) apte à être utilisé dans le cadre de la mise en œuvre de la technique proposée, dans un mode de réalisation particulier. Un tel terminal de communication (11) comprend un processeur sécurisé ayant accès à une mémoire sécurisée. Ce processeur sécurisé et cette mémoire sécurisée sont éventuellement distincts du processeur central et de la mémoire centrale qui régissent le fonctionnement courant du terminal de communication (prise en charge d'appel, d'envoi de messages, navigation sur Internet, exécution d'application courantes, etc.), et qui mettent en œuvre un environnement d'exécution courant (REE, de l'anglais « Rich Execution Environment ») du système d'exploitation installé sur le terminal de communication. Ce processeur et cette mémoire sécurisés – qui forment donc un espace sécurisé au sein du terminal de communication – peuvent par exemple être intégrés au sein d'un environnement d'exécution sécurisé (TEE, de l'anglais « Trusted Execution Environment ») qui est livré au fabricant de terminaux de communication. Cet environnement d'exécution sécurisé (TEE) peut par ailleurs être complété d'un module de sécurisation (SE, de l'anglais « Secure Element ») dont la fonction dans la cadre de la présente technique est de dialoguer avec un terminal de paiement virtuel. Un module de sécurisation (SE) se présente sous la forme d'une plate-forme matérielle résistante

aux attaques, au sein de laquelle peuvent être exécutées des applications sécurisées. Un tel module offre notamment un niveau de sécurisation supérieur à celui procuré par l'environnement d'exécution sécurisé (TEE), dans la mesure où il est conçu pour fournir une protection contre des attaques non seulement logicielles mais également matérielles (un environnement d'exécution sécurisé (TEE) étant conçu plus particulièrement pour offrir une protection contre des attaques logicielles, mais pas forcément contre des attaques matérielles). Plusieurs types de service (12) nécessitant l'obtention d'une autorisation pour la réalisation de transactions associées sont prédéfinis au sein de ce module de sécurisation (SE) (par exemple sous la forme d'applications spécifiques, également appelées applets). Afin de permettre à un utilisateur de pouvoir réaliser des transactions de paiement, le module de sécurisation (SE) intègre par exemple des types de services de paiement prédéfinis correspondant aux différents services de paiement les plus répandus. On peut citer à titre illustratif mais non limitatif les services de paiement Visa® et Mastercard®. D'autres types de services peuvent également être prédéfinis (La figure 1 présente à titre d'exemple un module de sécurisation (SE) au sein duquel sont prédéfinis quatre types de service 12.1 à 12.4, mais cet exemple est purement illustratif : un module de sécurisation selon la technique proposée intègre au moins un type de service). Chaque type de service prédéfini au sein d'un module de sécurisation est associé à un identifiant unique (PAN_S), construit sur le même format qu'un numéro de carte bancaire (ou PAN, de l'anglais « Primary Account Number »), c'est à dire selon la norme ISO/IEC 7812 (intitulée « Cartes d'identification - Identification des émetteurs »). Chacun de ces identifiants est non seulement unique au sein d'un même module de sécurisation, mais il est également unique au sein de l'ensemble des modules de sécurisation commercialisés. Ainsi, un tel module de sécurisation fourni à un fabricant de terminaux de communication contient, pour chaque type de service qui y est prédéfini, un identifiant qui fait office de signature unique et inaltérable et qui est construit sur le même format qu'un numéro de carte bancaire (quatre groupes de quatre chiffres). Au sein de ce module de sécurisation, chaque type de service est stocké sous la même forme que le sont les données contenues dans une carte à mémoire de type carte

bancaire (un type de service se comportant alors vis-à-vis de l'extérieur, comme une carte bancaire virtuelle avec son propre numéro (PAN_S)).

Comme décrit précédemment, les différents types de services permettant la réalisation de transactions associées peuvent prendre la forme d'applications spécifiques également appelées applets qui sont exécutées au sein du module de sécurisation (SE) du terminal de communication. Aussi, les différents types de service 12.1 à 12.4 présentés sur la figure 1 peuvent être assimilés à autant d'applets de traitement de transactions (12), aptes à traiter des données sécurisées selon les mêmes mécanismes que ceux mis en œuvre dans le cadre de la réalisation d'une transaction de paiement à partir d'une carte bancaire dans un mode « carte présente », en lien avec un terminal de paiement. Afin de garantir une sécurisation maximale lorsqu'une transaction est en cours, l'applet associée qui est exécutée au sein du module de sécurisation (applet de traitement de la transaction (12)) n'a pas la possibilité d'échanger des informations avec des composants du terminal de communication qui se situeraient en dehors du module de sécurisation (SE). On garantit ainsi un fonctionnement identique à celui d'une carte bancaire (qui ne peut échanger d'information qu'avec un terminal de paiement durant une transaction). Néanmoins, il peut s'avérer nécessaire ou utile pour l'applet de traitement de la transaction (12), au cours du processus de réalisation d'une transaction, d'avoir accès à certaines informations présentes en dehors du module de sécurisation (SE) du terminal de communication. A titre d'exemple, si l'utilisateur qui souhaite réaliser une transaction de paiement a provisionné plusieurs cartes bancaires dans son terminal de communication, il est nécessaire que le module de sécurisation (SE) soit en mesure de sélectionner la carte de paiement que l'utilisateur souhaite utiliser. Les différentes représentations des cartes qu'un utilisateur a à sa disposition (par exemple des images, des photos ou encore les quatre derniers numéros des cartes en question) ne sont pas nécessairement stockées au sein du module de sécurisation (SE) du terminal de communication (dont la quantité de mémoire n'est pas aussi élevée). Aussi, l'applet de traitement de la transaction (12) doit avoir la possibilité d'accéder à des informations externes, par exemple des informations contenues dans l'environnement d'exécution

courant (REE) ou dans l'environnement d'exécution sécurisé (TEE) du terminal de communication. Elle doit également avoir la possibilité d'accéder à des informations stockées au sein du module de sécurisation (SE) du terminal de communication, mais qu'elle ne contrôle pas directement.

Selon la technique proposée ici pour répondre à cette problématique, lorsqu'une transaction est en cours de traitement, une applet complémentaire (13) peut être exécutée au sein du module de sécurisation (SE), en parallèle de l'exécution de l'applet de traitement de la transaction (12). L'applet de traitement de la transaction (12) est en mesure de dialoguer (14) avec cette applet complémentaire (13), dans la mesure où toutes deux sont exécutées au sein du module de sécurisation (SE). En pratique, cet échange de données peut être réalisé au moyen d'interfaces logicielles dédiées. A titre d'illustration, un environnement d'exécution tel que celui proposé par Java Card®, couramment utilisé pour la mise en œuvre d'applications sur carte à puce, définit les modalités d'interaction entre les applets qui sont exécutées en son sein, et fourni notamment, sous l'appellation « Shareable interfaces », des moyens permettant l'échange de données inter applets. Dans cette solution, l'applet qui met des données à disposition au moyen d'une interface dédiée est en mesure d'autoriser ou non une autre applet à y accéder, sur la base d'un contrôle de son identifiant d'application (AID, de l'anglais « Application Identifier »). Les objets ainsi échangés entre l'applet de traitement de la transaction et l'applet complémentaire peuvent notamment prendre la forme de messages APDU (de l'anglais « Application Data Protocol Unit »), c'est à dire conformes au protocole de communication utilisé pour les échanges de données entre une carte à puce et un lecteur de carte à puce. L'applet complémentaire (13), qui n'est pas soumise aux mêmes contraintes de sécurisation et d'exécution temps-réel que l'applet de traitement des transactions, peut également échanger des données (15) avec des éléments du terminal de communication extérieurs au module de sécurisation, par exemple l'environnement d'exécution courant (REE) du terminal de communication ou encore l'environnement d'exécution sécurisé (TEE). Ainsi, l'applet complémentaire (13) est en mesure de récupérer toute donnée utile nécessaire à la poursuite d'une transaction, et de les communiquer à l'applet de traitement de la transaction (12).

L'applet complémentaire (13) peut également jouer d'autres rôles, en plus de celui de faire le lien entre l'applet de réalisation de la transaction (12) et les éléments extérieurs au module de communication. Elle peut par exemple contenir des informations représentatives des cartes provisionnées pour un type de service donné (par exemple un index permettant de distinguer plusieurs cartes de même catégorie), ou encore des informations de sécurisation supplémentaires, telles que des données biométriques concernant l'utilisateur. A titre d'illustration, de nombreux terminaux de communication sont maintenant équipés de capteurs capables de détecter et d'analyser une empreinte digitale. Selon une utilisation possible de la technique proposée, l'utilisateur qui dispose d'un tel terminal de communication a la possibilité – par exemple au moment où il décide d'activer un des types de services prédéfinis dans son terminal de communication (dans une phase dite de provisionnement) – d'opter pour une sécurisation renforcée des transactions, basée sur la vérification d'une empreinte digitale. S'il choisit cette option, l'utilisateur est alors invité à suivre une procédure de capture d'une empreinte digitale de référence au moyen du capteur dédié. Cette opération permet de délivrer une signature caractéristique de cette empreinte de référence, signature qui est ensuite stockée au sein de l'applet complémentaire, ou ailleurs dans le terminal de communication, par exemple au sein de l'environnement d'exécution sécurisé (TEE). Lors de la mise en œuvre ultérieure d'une transaction, l'applet de traitement de la transaction peut alors solliciter l'applet complémentaire, qui se charge de récupérer ladite signature associée à l'empreinte digitale de référence. L'applet complémentaire dispose de moyens d'échanges d'informations avec les autres environnements d'exécution du terminal de communication, extérieurs au module de sécurisation (notamment l'environnement de fonctionnement courant (REE) et l'environnement d'exécution sécurisé (TEE)), lui permettant d'accéder à cette signature de l'empreinte de référence, même si celle-ci n'est pas stockée en son sein. Dans ce contexte, l'applet complémentaire est utilisée pour obtenir une donnée nécessaire pour évaluer si la transaction peut être autorisée ou non : lorsqu'un utilisateur souhaite effectuer une transaction, il doit fournir, au moyen du capteur d'empreinte digitale de son terminal de communication, une empreinte courante également caractérisée par

une signature. La signature associée à l'empreinte de référence et la signature associée à l'empreinte courante sont alors transmises, sous une forme chiffrée, à au serveur de traitement de transactions qui se charge de les comparer. Ce mécanisme de sécurisation peut avantageusement remplacer ou venir compléter une saisie, par l'utilisateur, d'un numéro d'identification personnel (également appelé code PIN, de l'anglais « Personal Identification Number »)).

Dans un autre cas d'utilisation, l'applet complémentaire est utilisée pour obtenir des données relatives à la mise en œuvre d'un programme de fidélité (couramment appelé « fidelity program ») proposé par un site marchand, au moment où une transaction de paiement est réalisée auprès de ce site marchand. Par exemple, l'applet complémentaire est utilisée pour obtenir l'identifiant d'un utilisateur (usrId) auprès du site marchand, en fonction d'un identifiant dudit marchand (retId). Une association entre l'identifiant de marchand (retId) et l'identifiant de l'utilisateur (usrId) auprès de ce marchand a préalablement été stockée dans le terminal de communication, par exemple au moment d'un premier achat de l'utilisateur auprès de ce marchand, ou encore au moment de l'adhésion de l'utilisateur à un programme de fidélité proposé par ce marchand, à partir du terminal de communication.

Ainsi, lorsqu'un site marchand requiert auprès, d'un serveur de traitement de transactions, la création d'une transaction liée à la validation d'un panier d'achat par un utilisateur, il transmet, au serveur de traitement de transactions, son identifiant de marchand (retId). Le serveur de traitement de transactions instancie alors un terminal de paiement virtuel (VPOI) apte à communiquer avec le terminal de communication, et plus particulièrement avec l'applet de traitement de la transaction du module de sécurisation (SE) aux moyens d'APDU. Alternativement, le site marchand peut également réaliser seul l'instanciation du terminal de paiement virtuel et requérir l'établissement d'une session sécurisée avec le terminal de communication.

Quoi qu'il en soit, l'identifiant de marchand (retId) est ainsi transmis à l'applet de traitement de la transaction, qui interroge l'applet complémentaire afin de déterminer si l'utilisateur dispose d'un compte client auprès de ce marchand. L'applet complémentaire se charge donc de vérifier – au moyen d'une structure de données

hébergées en son sein ou ailleurs dans le terminal de communication – si une entrée correspondant à cet identifiant de marchand (retId) existe (l'utilisateur a déjà effectué des transactions auprès de ce marchand) et, le cas échéant, récupère l'identifiant de l'utilisateur auprès de ce marchand (usrId).

Cet identifiant d'utilisateur (usrId) est communiqué en retour à l'applet de traitement de la transaction, qui le transmet à son tour au marchand. Ce dernier peut alors consulter ses propres structures de données pour évaluer la situation de l'utilisateur associé, et les éventuels avantages auxquels il peut prétendre (créditer des points sur un programme de fidélité, bénéficier d'une réduction immédiate ou sur un prochain achat, etc.). Dans le cas où une réduction immédiate est proposée – octroyée par exemple au titre de la fidélité du client – le site marchand communique le nouveau montant (montant après réduction) au serveur de traitement de transactions qui le relaie à l'utilisateur via le terminal de paiement virtuel (VPOI). La réduction peut ainsi être immédiatement répercutée à l'utilisateur.

Selon la technique proposée, l'applet complémentaire est donc en charge de seconder au moins une applet de traitement de transactions, afin de lui fournir, à sa demande et au moment opportun, des données complémentaires ou bien nécessaires pour la poursuite de la transaction (par exemple des données biométriques), ou bien utiles pour enrichir la transaction (par exemple des données relatives à un programme de fidélité). Ces données peuvent être stockées au sein même de l'applet complémentaire, mais également ailleurs au sein du terminal de communication, notamment hors du module de sécurisation (SE), dans l'environnement d'exécution courant (REE) ou sécurisé (TEE) (l'applet complémentaire dispose alors de moyens de communication avec des applications exécutées au sein de ces environnements d'exécution). Dans un mode de réalisation particulier de la technique proposée, une même applet complémentaire peut être utilisée pour fournir des données complémentaires à l'ensemble des différentes applications de traitement de transactions susceptibles d'être exécutées au sein du terminal de communication. L'applet complémentaire intègre alors un mécanisme de gestion des autorisations, lui permettant de savoir si une applet de traitement de transaction a effectivement le droit

d'accéder à une donnée demandée (par exemple sur la base d'un identifiant (AID) de l'applet demandeuse). Alternativement, plusieurs applets complémentaires peuvent être exécutées au sein d'un même module de sécurisation, chacune étant dédiée à seconder une ou plusieurs autres applets de traitement de transactions bien identifiées.

5.2 Procédé associé

On décrit, en relation avec la **figure 2** et dans un mode de réalisation particulier de la technique proposée, un procédé de communication entre une première application de traitement de transactions et une deuxième application de traitement de données sécurisées, lesdites applications étant toute deux exécutées au sein d'un même module de sécurisation d'un terminal de communication. Un tel procédé est caractérisé en ce qu'il comprend :

- une étape de réception (21), par ladite première application, d'une requête en provenance d'un réseau de communication ;
- une étape de transmission (22), par ladite première application, d'une requête d'obtention d'une donnée sécurisée, à destination de ladite deuxième application ;
- une étape de vérification (23), par ladite deuxième application, que ladite première application est bien autorisée à accéder à ladite donnée requise ;

puis, lorsque ladite vérification s'avère positive :

- une étape d'obtention (24), par la deuxième application, de ladite donnée requise par la première application ;
- une étape de transmission (25), par ladite deuxième application, de ladite donnée requise, à destination de ladite première application ;
- une étape de transmission (26), par ladite première application, de ladite donnée requise à destination dudit réseau de communication.

L'étape de vérification (23), par la deuxième application, que la première application est bien autorisée à accéder à ladite donnée requise peut être réalisée en confrontant un identifiant (AID) de la première application (transmis par exemple dans la requête d'obtention de la donnée sécurisée) avec une liste d'identifiant d'applications effectivement autorisées à accéder à ladite donnée (liste d'identifiants qui est stockée

au sein de ladite deuxième application).

Comme déjà présenté dans les cas d'utilisation exposés précédemment, la donnée requise par la première application peut être stockée au sein d'un espace de stockage – de préférence sécurisé – de la deuxième application. Alternativement, elle peut être disponible au sein d'un environnement d'exécution du terminal de communication autre que le module de sécurisation (par exemple au sein de l'environnement d'exécution courant (REE) ou sécurisé (TEE) du terminal de communication). Dans ce dernier cas, la deuxième application est apte à émettre à son tour, à destination d'applications tierces exécutées au sein de l'environnement d'exécution idoine, une requête d'obtention de la donnée requise par la première application. La donnée ainsi récupérée peut alors être par exemple temporairement stockée au sein de l'espace de stockage de la deuxième application, avant d'être relayée vers la première application. Dans ce cas, la deuxième application peut alors contenir une liste d'identifiants d'applications autorisées à enregistrer des données au sein de son espace de stockage.

5.3 Dispositif

On décrit, en relation avec la **figure 3**, un module de sécurisation d'un terminal de communication comprenant des moyens permettant l'exécution du procédé décrit préalablement.

Par exemple, le module de sécurisation comprend une mémoire 31 constituée d'une mémoire tampon, une unité de traitement 32, équipée par exemple d'un microprocesseur, et pilotée par le programme d'ordinateur 33, mettant en œuvre nécessaires à la mise en œuvre des fonctions de vérification.

À l'initialisation, les instructions de code du programme d'ordinateur 33 sont par exemple chargées dans une mémoire avant d'être exécutées par le processeur de l'unité de traitement 32. L'unité de traitement 32 reçoit en entrée (I) par exemple une requête de demande de traitement d'une transaction, en provenance d'un réseau de communication. Le microprocesseur de l'unité de traitement 32 met en œuvre les étapes du procédé de communication entre une première application de traitement de transactions et une deuxième application de traitement de données sécurisées, selon les

instructions du programme d'ordinateur 33 pour permettre l'obtention d'une donnée sécurisée contribuant au traitement de la transaction, et notifier en sortie (T) le résultat de ce traitement.

Pour cela, le module de sécurisation comprend, outre la mémoire tampon 31, des moyens d'interface avec un réseau de communication, et des moyens d'interface avec d'autres environnements d'exécution présents au sein du terminal de communication. Le module de sécurisation comprend également des moyens de traitement cryptographiques ; ces moyens de traitement comprennent par exemple un processeur de chiffrement dédié et des clés de chiffrement, comme des clés de session dérivée d'une clé initiale.

Ces moyens peuvent être pilotés par le processeur de l'unité de traitement 32 en fonction du programme d'ordinateur 33.

REVENDICATIONS

1. Module de sécurisation (SE) intégré au sein d'un terminal de communication mobile (11), module caractérisé en ce qu'il comprend

au moins une première application (12) de traitement de transaction comprenant au moins une interface de communication avec un réseau de communication de manière sécurisée, et

au moins une deuxième application (13) de traitement de données sécurisées comprenant au moins une interface de communication avec un environnement d'exécution dudit terminal de communication,

ladite première application (12) étant en mesure de requérir au moins une donnée auprès de ladite deuxième application (13).

2. Module de sécurisation selon la revendication 1, caractérisé en ce que ladite deuxième application comprend au moins un espace de stockage sécurisé.

3. Module de sécurisation selon la revendication 1, caractérisé en ce que ladite deuxième application comprend au moins une liste d'identifiants d'applications autorisées à accéder à ladite au moins une donnée.

4. Module de sécurisation selon la revendication 1,, caractérisé en ce que ladite deuxième application comprend au moins une liste d'identifiants d'applications autorisées à requérir la mémorisation de données au sein dudit espace de stockage sécurisé.

5. Module de sécurisation selon la revendication 1, caractérisé en ce que ladite au moins une donnée appartient au groupe comprenant :

- une donnée représentative d'une carte de paiement ;
- une donnée représentative d'une association entre un identifiant de marchand d'une part, et un identifiant d'un utilisateur auprès dudit marchand d'autre

part ;

- une donnée d'identification ou d'authentification biométrique.

6. Procédé de communication entre une première application de traitement de transactions et une deuxième application de traitement de données sécurisées, lesdites applications étant exécutées au sein d'un module de sécurisation d'un terminal de communication, procédé caractérisé en ce qu'il comprend :

- une étape de réception, par ladite première application, d'une requête en provenance d'un réseau de communication ;
- une étape de transmission, par ladite première application, d'une requête d'obtention d'une donnée sécurisée, à destination de ladite deuxième application ;
- une étape d'obtention, par ladite deuxième application, de ladite donnée requise par la première application ;
- une étape de transmission, par ladite deuxième application, de ladite donnée requise, à destination de ladite première application ;
- une étape de transmission, par ladite première application, de ladite donnée requise à destination dudit réseau de communication.

7. Procédé selon la revendication 6 caractérisé en ce qu'il comprend, préalablement à ladite étape d'obtention, par ladite deuxième application, de ladite donnée requise par la première application, une étape de vérification, par ladite deuxième application, que ladite première application est bien autorisée à accéder à ladite donnée requise.

8. Procédé selon la revendication 6 caractérisé en ce que ladite étape d'obtention, par ladite deuxième application, de ladite donnée requise par la première application, comprend les sous-étapes suivantes :

- transmission d'une requête d'obtention de ladite donnée à destination d'un environnement d'exécution dudit terminal de communication ;

- réception de ladite donnée requise par la première application, en provenance dudit environnement d'exécution dudit terminal de communication.

9. Produit programme d'ordinateur téléchargeable depuis un réseau de communication et/ou stocké sur un support lisible par ordinateur et/ou exécutable par un microprocesseur, caractérisé en ce qu'il comprend des instructions de code de programme pour l'exécution d'un procédé de communication selon l'une quelconque des revendications 7 et 8, lorsqu'il est exécuté sur un ordinateur.

1/1

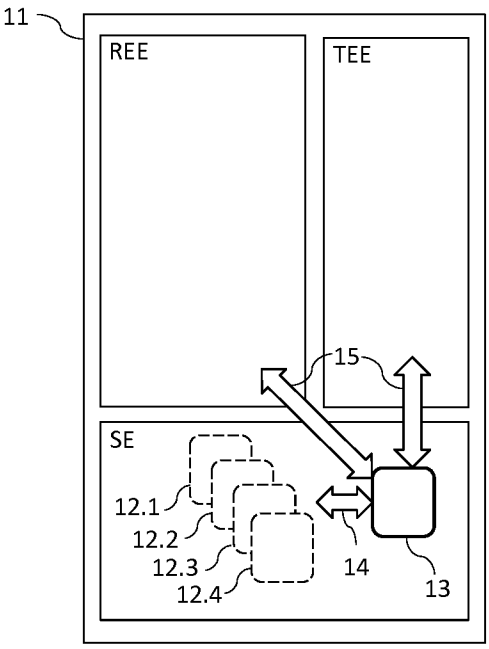

Fig. 1

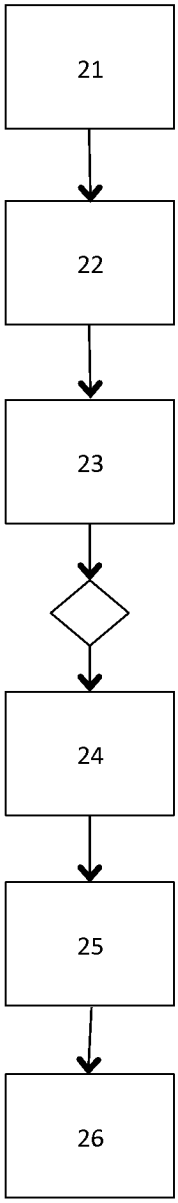

Fig. 2

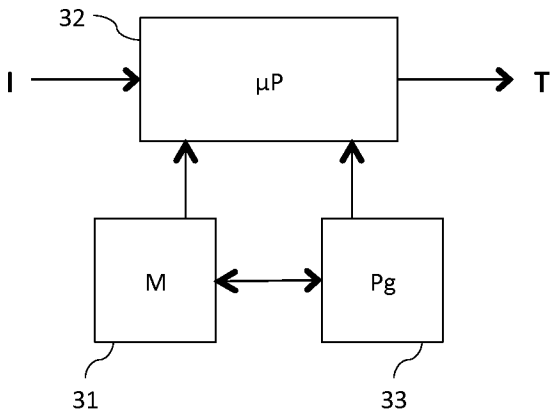

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2016/050318

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q20/34 G06Q20/42 H04L29/06 G06Q20/32 H04W12/08
G06F21/53
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 H04L H04W G06F

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2011/078081 A1 (PIRZADEH KIUSHAN [US] ET AL) 31 March 2011 (2011-03-31) paragraph [0027] - paragraph [0031] paragraph [0037] - paragraph [0060] figures 2, 3	1-9
A	US 2014/317686 A1 (VETILLARD ERIC [FR]) 23 October 2014 (2014-10-23) abstract paragraph [0032] - paragraph [0050]	1-9
A	EP 2 746 981 A1 (ST ERICSSON SA [CH]) 25 June 2014 (2014-06-25) abstract paragraph [0030] - paragraph [0037]	1-9

-/--

[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
10 March 2016	17/03/2016

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	Bertolissi, Edy

1

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.
A	"EMV Mobile Contactless Payment: Technical Issues and Position Paper", INTERNET CITATION, 1 October 2007 (2007-10-01), pages 1-37, XP007908266, Retrieved from the Internet: URL:http://www.emvco.com/mobile.aspx [retrieved on 2009-04-20] Section 1.4 -----	1-9

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2016/050318

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011078081 A1	31-03-2011	AU 2010300674 A1	26-04-2012
		CA 2776438 A1	07-04-2011
		CN 102656599 A	05-09-2012
		EP 2483854 A2	08-08-2012
		RU 2012117227 A	10-11-2013
		US 2011078081 A1	31-03-2011
		WO 2011041447 A2	07-04-2011
US 2014317686 A1	23-10-2014	NONE	
EP 2746981 A1	25-06-2014	NONE	

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2016/050318

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06Q20/34 G06Q20/42 H04L29/06 G06Q20/32 H04W12/08
G06F21/53
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 H04L H04W G06F

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

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

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 2011/078081 A1 (PIRZADEH KIUSHAN [US] ET AL) 31 mars 2011 (2011-03-31) alinéa [0027] - alinéa [0031] alinéa [0037] - alinéa [0060] figures 2, 3	1-9
A	US 2014/317686 A1 (VETILLARD ERIC [FR]) 23 octobre 2014 (2014-10-23) abrégé alinéa [0032] - alinéa [0050]	1-9
A	EP 2 746 981 A1 (ST ERICSSON SA [CH]) 25 juin 2014 (2014-06-25) abrégé alinéa [0030] - alinéa [0037]	1-9

-/--

[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
10 mars 2016	17/03/2016

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	Bertolissi, Edy

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	"EMV Mobile Contactless Payment: Technical Issues and Position Paper", INTERNET CITATION, 1 octobre 2007 (2007-10-01), pages 1-37, XP007908266, Extrait de l'Internet: URL:http://www.emvco.com/mobile.aspx [extrait le 2009-04-20] Section 1.4 -----	1-9

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/EP2016/050318

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2011078081 A1	31-03-2011	AU 2010300674 A1	26-04-2012
		CA 2776438 A1	07-04-2011
		CN 102656599 A	05-09-2012
		EP 2483854 A2	08-08-2012
		RU 2012117227 A	10-11-2013
		US 2011078081 A1	31-03-2011
		WO 2011041447 A2	07-04-2011
US 2014317686 A1	23-10-2014	AUCUN	
EP 2746981 A1	25-06-2014	AUCUN	