(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 031 610***

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **15 50193**

(51) Int Cl[8] : ***G 06 F 21/30*** *(2016.01)*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 09.01.15.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 15.07.16 Bulletin 16/28.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Ce dernier n'a pas été établi à la date de publication de la demande.*

(60) **Références à d'autres documents nationaux apparentés :**

( ) **Demande(s) d'extension :**

(71) **Demandeur(s) :** *COMPAGNIE INDUSTRIELLE ET FINANCIERE D'INGENIERIE "INGENICO"* — FR.

(72) **Inventeur(s) :** QUENTIN PIERRE.

(73) **Titulaire(s) :** COMPAGNIE INDUSTRIELLE ET FINANCIERE D'INGENIERIE "INGENICO".

(74) **Mandataire(s) :** CABINET PATRICE VIDON.

(54) PROCEDE DE TRAITEMENT D'UNE TRANSACTION A PARTIR D'UN TERMINAL DE COMMUNICATION.

(57) Module de sécurisation (SE) intégré au sein d'un terminal de communication mobile, module caractérisé en ce qu'il comprend au moins une première application de traitement de données sécurisée comprenant au moins une interface de communication avec un environnement d'exécution non sécurisé et au moins une deuxième application de traitement de données sécurisée comprenant au moins une interface de communication avec un réseau de communication de manière sécurisée, ladite deuxième application étant en mesure de requérir au moins une donnée auprès de ladite première application.

FR 3 031 610 - A1

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. La technique proposée se rapporte 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 limitées et ne concerne 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).

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

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 présente un synoptique de la technique proposée ;

5. Description

La technique proposée ne présente pas au moins certains de ces problèmes de l'art antérieur. En effet, il est proposé ici un procédé d'obtention d'une autorisation nécessaire à la réalisation d'une transaction effectuée à partir d'un terminal de communication. On entend ici le terme « transaction » au sens large : il peut s'agir aussi bien d'une transaction financière (par exemple une transaction de paiement), que d'une transaction de tout autre nature, telle que la publication ou la suppression de commentaires sur un réseau social en ligne, ou tout autre transaction nécessitant l'obtention d'une autorisation pour être réalisée.

Le principe général de la technique proposée consiste à s'appuyer sur 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 », et à reprendre ces mécanismes dans le but d'obtenir une autorisation pour la réalisation d'une transaction quelconque (pas seulement des transactions de paiement) à partir d'un terminal de communication.

Un terminal de communication selon la technique proposée comprend un processeur sécurisé ayant accès à une mémoire sécurisée. Il est important de noter ici que ce processeur sécurisé et cette mémoire sécurisée sont dédiés à la réalisation de transactions, et qu'ils sont 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, etc.). 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 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) dont la fonction dans la cadre de la présente technique est de dialoguer avec un terminal de paiement virtuel. Plusieurs types de service nécessitant l'obtention d'une autorisation pour la réalisation de transactions associées sont prédéfinis au sein de ce module de sécurisation (par exemple sous la forme d'applications spécifiques, également appelées applets). Des exemples de tels types de service sont : paiement Visa®, paiement Mastercard®, service lié à un réseau social en ligne donné, etc. 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 »). 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. 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 du terminal de communication. Afin de garantir une sécurisation

maximale lorsqu'une transaction est en cours, l'applet associée alors exécutée au sein du module de sécurisation (applet de réalisation de la transaction) 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. En effet, le processeur central du terminal de communication ne doit en effet pas être en mesure d'agir sur la manière dont le module de sécurisation fonctionne. Néanmoins, il peut s'avérer nécessaire pour l'applet de réalisation de la transaction, au cours du processus de réalisation d'une transaction, d'avoir accès à certaines informations présentes en dehors du module de sécurisation 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 soit en mesure de lui proposer de choisir la carte de paiement qu'il souhaite utiliser. Les différentes représentations des cartes qu'un utilisateur a à sa disposition (par exemple des images ou des photos des cartes en question) ne sont pas nécessairement stockées au sein du module de sécurisation du terminal de communication. Aussi, l'applet de réalisation de la transaction doit avoir la possibilité d'accéder à des informations externes, par exemple des informations contenues dans la mémoire centrale du terminal de communication ou dans l'environnement d'exécution sécurisé (TEE).

Selon la technique proposée ici pour répondre à cette problématique, lorsqu'une transaction est en cours, une applet complémentaire est exécuté au sein du module de sécurisation, en parallèle de l'exécution de l'applet de réalisation de la transaction. L'applet de réalisation de la transaction est en mesure de dialoguer avec cette applet complémentaire, dans la mesure où toutes deux sont exécutées au sein du module de sécurisation. Cette applet complémentaire, qui n'est pas soumise aux mêmes contraintes de sécurisation et d'exécution temps-réel que le programme de gestion des transactions, peut quant à elle échanger des données avec des éléments du terminal de communication extérieurs au module de sécurisation, par exemple le processeur

central du terminal de communication ou encore l'environnement d'exécution sécurisé (TEE). Ainsi, l'applet complémentaire est en mesure de récupérer toute donnée utile nécessaire à la poursuite d'une transaction, et de les communiquer à l'applet de réalisation de la transaction. L'applet complémentaire peut également jouer d'autres rôles, en plus de celui de faire le lien entre l'applet de réalisation de la transaction et les éléments extérieurs au module de communication. Elle peut par exemple contenir des informations de sécurisation supplémentaires, telles que des données biométriques concernant l'utilisateur, ou encore diverses informations concernant les cartes provisionnées pour un type de service donné (notamment un index utile pour distinguer plusieurs cartes de même catégorie).

Dispositifs de mises en œuvre.

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

Par exemple, le terminal de communication comprend une mémoire 51 constituée d'une mémoire tampon, une unité de traitement 52, équipée par exemple d'un microprocesseur, et pilotée par le programme d'ordinateur 53, mettant en œuvre nécessaires à la mise en œuvre des fonctions de vérification.

À l'initialisation, les instructions de code du programme d'ordinateur 53 sont par exemple chargées dans une mémoire avant d'être exécutées par le processeur de l'unité de traitement 52. L'unité de traitement 52 reçoit en entrée par exemple une notification. Le microprocesseur de l'unité de traitement 52 met en œuvre les étapes du procédé de création, selon les instructions du programme d'ordinateur 53 pour permettre la saisie d'un code d'autorisation (un code PIN par exemple).

Pour cela, le dispositif comprend, outre la mémoire tampon 51, des moyens d'affichage et de saisie ; ces moyens peuvent se présenter sous la forme d'un processeur ou d'un ensemble de ressources sécurisées permettant de

sécuriser la saisie de l'autorisation. Le dispositif 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 52 en fonction du programme d'ordinateur 53.

REVENDICATIONS

1. Module de sécurisation (SE) intégré au sein d'un terminal de communication mobile, module caractérisé en ce qu'il comprend au moins une première application de traitement de données sécurisée comprenant au moins une interface de communication avec un environnement d'exécution non sécurisé et au moins une deuxième application de traitement de données sécurisée comprenant au moins une interface de communication avec un réseau de communication de manière sécurisée, ladite deuxième application étant en mesure de requérir au moins une donnée auprès de ladite première application.