(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 905 187**

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

(21) **N° d'enregistrement national :** **06 07440**

(51) Int Cl[8] : **G 06 F 21/00** (2006.01), G 07 C 9/00

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 22.08.06.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 29.02.08 Bulletin 08/09.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

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

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

(72) **Inventeur(s) :** NACCACHE DAVID.

(73) **Titulaire(s) :**

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

(54) TERMINAL DE PAIEMENT ELECTRONIQUE BIOMETRIQUE ET PROCEDE DE TRANSACTION.

(57) L'invention concerne un terminal de paiement électronique, comprenant des moyens d'acquisition de données biométriques et un programme adapté à:

- acquérir des données biométriques lors d'une transaction par l'intermédiaire des moyens d'acquisition de données biométriques; et
- stocker les données biométriques dans le terminal.

L'invention concerne également un procédé de transaction correspondant.

FR 2 905 187 - A1

TERMINAL DE PAIEMENT ELECTRONIQUE BIOMETRIQUE ET PROCEDE DE TRANSACTION

La présente invention concerne un terminal de paiement électronique. L'invention concerne également un procédé de transaction correspondant.

Un terminal de paiement électronique (TPE) est un appareil électronique permettant d'enregistrer une transaction de paiement sécurisée. Un TPE est typiquement un ordinateur placé chez un commerçant, qui permet des règlements par cartes bancaires (telles que les cartes à puce ou les cartes à piste magnétique). Le commerçant introduit la carte de son client dans le lecteur du terminal et entre le montant de la transaction. Le client valide son achat, par exemple en composant son code confidentiel sur le clavier de l'appareil et reçoit un ticket confirmant la transaction.

Certains TPE sont portatifs; ils comprennent notamment un lecteur de carte à puce, des moyens d'impression de ticket, un modem, et une carte GSM. Ils sont utilisés notamment dans les taxis, les marchés, ou pour la livraison à domicile.

Ces TPE sont souvent reliés chez les commerçants à des moyens de gestion (par exemple une caisse enregistreuse) qui permet d'assurer la gestion du point de vente. Le système TPE/moyen de gestion constitue un terminal point de vente (TPV). Certains TPE comportent une partie portative pour la lecture des cartes à puce et l'impression des tickets. Cette partie repose sur un socle lorsqu'elle n'est pas utilisée, et communique avec ce socle par une liaison sans fil, par exemple radioélectrique, en utilisation. Le socle peut être connecté au moyen de gestion; il comprend typiquement un modem permettant d'obtenir des autorisations de prélèvement d'organismes habilités.

Bien que le système de paiement par TPE présente un niveau élevé de sécurité grâce à l'identification de la carte bancaire par puce et / ou bande magnétique, à l'utilisation éventuelle d'un code d'utilisateur (code PIN) et à l'utilisation éventuelle d'une signature, des fraudes restent possibles en cas de vol de carte bancaire et de vol de code PIN par exemple. Il est donc souhaitable d'une part d'améliorer encore le niveau de sécurité en rendant la fraude plus dissuasive ; et d'autre part éventuellement de permettre une vérification ultérieure de l'identité de l'utilisateur à l'origine de la transaction.

Ces problèmes se posent en termes similaires pour d'autres terminaux électroniques tels que les distributeurs automatiques de billets par exemple.

L'invention a par conséquent pour but de concevoir des terminaux dotés d'un système décourageant la fraude.

L'invention a ainsi pour objet un terminal de paiement électronique comprenant des moyens d'acquisition de données biométriques et un programme adapté à :

– acquérir des données biométriques lors d'une transaction par l'intermédiaire des moyens d'acquisition de données biométriques ; et

– stocker les données biométriques dans le terminal de paiement.

Dans des modes de réalisation préférés, l'invention comprend une ou plusieurs des caractéristiques suivantes :

- le programme est en outre adapté à requérir auprès d'un central une autorisation de validation de la transaction et le cas échéant, à recevoir du central l'autorisation de validation de la transaction et valider la transaction;

- le programme est en outre adapté à stocker les données biométriques dans le terminal définitivement ou pendant une durée déterminée et à fournir les données biométriques stockées, le cas échéant pendant la durée déterminée, et de préférence sous réserve que certaines conditions de sécurité soient satisfaites;

- le programme est en outre adapté à fournir les données biométriques au central avant de requérir l'autorisation de validation de la transaction ou simultanément;

- le programme est en outre adapté à recevoir du central des données biométriques de référence, établir une comparaison des données biométriques acquises aux données biométriques de référence ; et valider ou non la transaction en fonction du résultat de la comparaison;

- le programme est en outre adapté à établir une comparaison des données biométriques avec des données type ; et le cas échéant, en fonction du résultat de la comparaison, ne pas valider la transaction ou acquérir de nouvelles données biométriques par l'intermédiaire des moyens d'acquisition de données biométriques;

- le programme est en outre adapté à établir la comparaison des données biométriques aux données biométriques de référence et / ou la comparaison des données biométriques aux données type par reconnaissance de forme;

- le terminal de paiement électronique selon l'invention comprend en outre des moyens de saisie d'un code par un utilisateur, et le programme est configuré de sorte que les moyens d'acquisition de données biométriques font office pour l'utilisateur de moyens de validation de la saisie du code;

- les moyens d'acquisition de données biométriques sont choisis parmi les appareils photographiques permettant la capture d'images fixes ou mouvantes, les capteurs d'empreintes digitales, les capteurs de la forme de l'iris; et

- le programme est en outre adapté à chiffrer des données biométriques au sein du terminal à l'aide d'un algorithme de chiffrement probabiliste à clé publique, la clé

publique appartenant à l'une des entités suivantes : la banque, le propriétaire de la carte, un tiers de confiance ou le fabriquant du terminal.

L'invention concerne également un procédé de transaction comprenant l'acquisition par un terminal de paiement électronique de données biométriques lors d'une transaction et le stockage des données biométriques dans le terminal de paiement. Selon une variante, ce procédé est mis en œuvre avec le terminal de paiement électronique selon l'invention. Selon une autre variante, ce procédé comprend en outre une étape de validation de la transaction indépendamment des données biométriques stockées.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description détaillée qui suit des modes de réalisation de l'invention, donnés à titre d'exemple uniquement.

Dans la suite de la description, on prend pour exemple de terminal électronique selon l'invention un terminal de paiement électronique (TPE). Ce mode de réalisation est avantageux car il est souhaitable d'améliorer la confiance des utilisateurs (clients et commerçants) dans le système du paiement par TPE. En outre, l'application de l'invention à un TPE est d'autant plus avantageuse que le nombre de transaction effectuée grâce aux TPEs est important.

L'invention propose un TPE comprenant des moyens d'acquisition de données biométriques.

Par données biométriques on entend des données relatives aux caractéristiques physiques des personnes humaines. Les données biométriques peuvent être par exemple relatives aux empreintes digitales, à la forme du visage, à la forme de l'iris de l'œil, une simple photographie ou autres.

A cet égard, il est important de noter que les données biométriques dont il est question dans la présente invention ne doivent pas être nécessairement analysables ou compréhensibles par une machine mais peuvent être des données dont l'analyse où la reconnaissance demande une intervention humaine (e.g. une photographie) ou celle d'un expert humain. L'intervention humaine, dans la mesure où elle n'est exigée qu'a posteriori, par exemple en cas de fraude avérée (c'est-à-dire relativement rarement), peut s'avérer plus simple à mettre en œuvre.

Les moyens d'acquisition des données biométriques peuvent être tout capteur de données biométriques, par exemple un capteur d'empreintes digitales ou un appareil photographique ou encore une combinaison de différents capteurs et / ou appareils photographiques. Des dispositifs d'acquisition d'image spécifique (appliqués au visage ou aux empreintes), de données iriennes, et des dispositifs d'enregistrement de la voix sont connus. L'acquisition d'empreintes digitales est tout particulièrement bien adaptée aux terminaux de paiement car elle ne bouleverse pas

les habitudes de l'utilisateur, habitué à utiliser ses doigts avec un tel terminal. L'acquisition d'images numériques peut par ailleurs être envisagée au moyen de dispositifs similaires à ceux que l'on trouve aujourd'hui communément dans les téléphones portables ou des caméras de surveillance bon marché. Ainsi, par données biométriques, nous entendons également un film pris par le TPE, par exemple au format MPEG.

Le TPE comprend également un programme, mémorisé dans l'unité centrale du TPE. Ce programme fait par exemple partie du système d'exploitation du TPE ou est ajouté (installé) par-dessus le système d'exploitation. Le programme est adapté à acquérir des données biométriques lors d'une transaction, c'est-à-dire à mettre en œuvre les moyens d'acquisition de données biométriques, ainsi qu'à stocker les données biométriques après acquisition. Le stockage peut se faire de manière transitoire (dans la mémoire vive) ou durable, voire définitive, selon les modes de réalisation.

Par transaction on entend une opération de modification de données, typiquement dans une ou plusieurs bases de données et dispositifs. Cette modification peut par exemple se faire hors ligne (dans la carte et/ou le TPE seulement), en ligne (au niveau du central) ou selon un mode mixte. Dans le cas du TPE, la transaction est un paiement.

Selon un mode de réalisation préféré, la validation de la transaction n'est soumise à aucun contrôle par le TPE (et le central, éventuellement) des données biométriques acquises, préalablement à la transaction. Il est ainsi possible, pour un utilisateur, de prêter sa carte bancaire, par exemple à un conjoint ou ami, sans risque de blocage de la transaction.

De préférence, le TPE est relié à un central via des moyens de communication avec le central. Le programme peut par exemple être adapté à requérir auprès du central une autorisation de validation de la transaction. Cette requête s'accompagne de la transmission de données au central. En particulier, dans le cas d'une transaction de paiement, les données peuvent comprendre des données relatives au marchand, à l'identification du compte bancaire de l'utilisateur payeur et des données relatives à la somme d'argent qui est l'objet de la transaction. Une fois ces données traitées par le central, le central transmet au TPE une autorisation ou une non-autorisation de validation de la transaction. Le programme du TPE est alors adapté pour recevoir éventuellement l'autorisation ou la non-autorisation de validation de la transaction et pour valider la transaction en cas de réception d'une autorisation de validation (ou pour ne pas valider la transaction en cas d'absence de réception d'autorisation de validation ou en cas de réception d'une non-autorisation de validation). Pour plus de précisions, on se reportera par exemple au "Manuel du paiement électronique" et au

"Protocole de Transmission avec les Centres de Traitement et d'Autorisation" édités par le Groupement des Cartes Bancaires "CB".

Selon un mode de réalisation particulier, le programme est adapté à stocker de manière durable dans le TPE les données biométriques acquises. Ce stockage peut être effectué dans un bloc mémoire vive dont le contenu est maintenu par une batterie ou dans une mémoire flash, disque dur, etc. Ce stockage peut être assuré de manière définitive ou seulement pendant une durée déterminée en fonction de la configuration du programme. Cette durée peut être par exemple d'une semaine, d'un mois ou d'un an. Eventuellement, le programme est adapté à effacer les données biométriques une fois la durée déterminée écoulée ou encore selon un principe de premier entré, premier sorti.

Le programme peut en outre être adapté à fournir à la demande les données biométriques stockées pendant la durée de stockage. Evidemment, une telle fourniture de données biométriques serait typiquement soumise à la satisfaction de certaines conditions de sécurité telles que la présentation d'un code PIN ou l'insertion dans le terminal d'une « carte administrateur ». Ainsi les données biométriques stockées sont par exemple disponibles pour la police et la justice si une contestation est soulevée quant à l'identité de l'utilisateur du TPE (le payeur en l'occurrence) ou si une fraude est avérée après la transaction. L'exploitation des données biométriques stockées permet de vérifier si l'utilisateur était ou non une personne autorisée à effectuer la transaction et permet éventuellement de suivre à la trace un fraudeur, voire de déterminer l'identité de l'utilisateur non autorisé. Il faut noter que ce mode de réalisation permet, si on le souhaite, de prévoir que la validation de la transaction s'effectue indépendamment des données biométriques acquises. Dans ce cas, les données biométriques sont acquises pendant la transaction mais n'interviennent pas dans le processus de validation de la transaction, elles restent simplement disponibles pour une exploitation ultérieure, en cas de problème. En minimisant les occasions d'exploitation effective des données biométriques, ce mode de réalisation offre des garanties particulières en termes de respect de la vie privée et des libertés individuelles.

Selon un autre mode de réalisation, le programme est adapté à fournir les données biométriques acquises au central. Dans ce cas, on peut prévoir que le TPE ne stocke les données biométriques que de manière transitoire et les efface ensuite. Les données biométriques peuvent par exemple être conservées au niveau du central en vue d'une utilisation ultérieure de manière analogue à ce qui a été décrit ci-dessus. Les données biométriques peuvent également être, dans des cas exceptionnels, immédiatement traitées par le central de manière à identifier l'utilisateur du TPE, par exemple en cas de doute ou de risque particulier sur la transaction (par exemple : un

montant important ou un achat dans un pays lointain). Dans ce cas, le résultat de l'analyse des données biométriques, éventuellement en complément de celle d'autres données telles qu'un code PIN ou des données propres au moyen de paiement (carte bancaire), conditionne en partie la transmission ou non par le central d'une autorisation ou d'une non-autorisation de validation de transaction.

L'analyse des données biométriques consiste par exemple à comparer les données biométriques à des données biométriques de référence, par exemple associées au ou aux utilisateur(s) autorisés du moyen de paiement. Il y a donc identification formelle de l'utilisateur avant la transaction (mais, de préférence, en des cas exceptionnels seulement), ce qui rend la fraude (et la contestation) impossible ou extrêmement difficile. Comme de tels cas de risque particulier devraient normalement être plutôt rares, la mise en œuvre du système ne demande pas de calculs lourds et ne ralentit pas la fluidité d'opérations de caisse. Ceci s'avère d'autant plus avantageux que le nombre de passages de clients par heure augmente.

Selon une variante, et toujours (de préférence) en cas de risque particulier sur la transaction, la comparaison des données biométriques aux données biométriques de référence peut s'effectuer au niveau du TPE. Dans ce cas, le central fournit par exemple au TPE les données biométriques de référence (associées au moyen de paiement utilisé dans la transaction demandée). Ces données de référence peuvent alternativement être lues directement dans la carte bancaire ou la SIM de l'utilisateur. Alternativement, ces données de référence peuvent provenir de toute source de stockage digne de confiance y compris la mémoire du TPE lui-même. Le TPE valide ou non la transaction en fonction du résultat de cette comparaison, c'est-à-dire que la transaction est validée si les données biométriques acquises sont jugées concordantes avec les données biométriques de référence.

Après validation de la transaction, on peut, selon une variante, prévoir l'effacement des données biométriques et des données biométriques de référence au niveau du terminal afin de garantir la confidentialité des données biométriques.

Dans les modes décrits ci-dessus, l'analyse des données biométriques peut faire intervenir une reconnaissance de forme automatisée (par exemple reconnaissance de la forme d'une empreinte digitale, d'un iris, d'un visage) ou humaine (visualisation de la photographie en temps réel par un employé de banque connaissant l'utilisateur légitime de la carte), auxquels cas les données biométriques de référence sont représentatives d'une forme d'empreinte digitale, d'iris ou de visage d'un ou plusieurs utilisateurs autorisés associés au moyen de paiement.

Selon un mode de réalisation particulier, le programme est également adapté à s'assurer que les données acquises sont bel et bien exploitables. Pour ce faire, il établit une comparaison des données biométriques avec des données type

(éventuellement par reconnaissance de forme). Ainsi, le cas échéant, en fonction de leur exploitabilité, le programme peut être configuré pour ne pas valider la transaction ou requérir et acquérir de nouvelles données biométriques par l'intermédiaire des moyens d'acquisition de données biométriques. En d'autres termes, le programme est adapté à vérifier si les données acquises présentent bien la forme caractéristique nécessaire à leur exploitation. Par exemple, si les données biométriques correspondent à une empreinte digitale, le programme est adapté à rechercher dans l'image obtenue lors de l'acquisition de données les caractéristiques typiques d'une empreinte digitale quelconque afin de vérifier si les données biométriques acquises correspondant à l'empreinte digitale sont exploitables. Si ce n'est pas le cas, par exemple parce que l'utilisateur porte un gant, le programme, selon la configuration retenue, ne valide pas la transaction ou est adapté à acquérir de nouvelles données biométriques (par exemple après requête en ce sens). La procédure peut être répétée si les nouvelles données biométriques ne sont toujours pas satisfaisantes. La même procédure peut s'appliquer dans le cas de la reconnaissance de la forme d'un visage ou de la forme d'un iris, afin d'éviter que soit traitée une image où n'apparaît pas correctement le visage ou l'iris de l'utilisateur. Ainsi, on peut faire en sorte qu'il soit impossible à l'utilisateur du TPE de se soustraire à l'acquisition de données biométriques exploitables pour effectuer la transaction.

Ainsi, dans le TPE seraient par exemple conservées pour audit ultérieur des structures de données {T,B} où T est la référence de la transaction (par exemple le numéro de transaction) et B est les données biométriques acquises lors de la transaction. Aussi, il est possible d'enrichir les structures de données sauvegardées dans le TPE avec des champs supplémentaires, non remontés au central mais sauvegardés afin de faciliter une enquête ultérieure. De telles données additionnelles (notées D et généralisant les structures de données {T,B} en {T,B,D}) sont par exemple une photographie du bien acheté, une copie électronique du contenu du ticket de caisse, l'identité du cassier ayant effectué la vente et pouvant potentiellement témoigner plus tard etc.).

Un mode d'encodage particulièrement avantageux et naturel consisterait à encoder l'image de l'empreinte digitale dans un fichier graphique nommé T.jpg. Ainsi l'information B est le fichier T.jpg et il n'y a pas besoin de créer une base de données proprement dite.

Aussi, dans le cas ou les données seraient remontées vers le central, il est à noter que la transmission de T et de B (ou {B,D}) peut ne pas avoir lieu en même temps. Ainsi, T peut être transmis en temps réel alors que l'ensemble des B (ou

{B, D}) accumulés durant la journée pourrait être remonté vers la central durant la nuit. Ceci permet de raccourcir la durée de la transaction.

Enfin, l'on notera que la transaction peut s'effectuer de manière concurrente (simultanée) avec la capture de l'information biométrique. Ceci permet d'optimiser le temps de passage en caisse.

De plus, l'archivage de la donnée biométrique peut être conditionné à l'accord préalable de l'utilisateur légitime. Dans ce mode de réalisation, lors de l'obtention du moyen de paiement (typiquement carte de crédit), l'utilisateur choisit librement d'associer (ou pas) une sauvegarde biométrique à sa carte. Ainsi, lorsqu'un TPE entre en contact avec la carte, il contacte le central qui avant de valider la transaction consulte sa base de données afin de déterminer si l'utilisateur a souscrit ou pas la sauvegarde biométrique. Dans l'affirmative, le central notifie cela au terminal qui ne validera pas la transaction avant d'avoir procédé à l'acquisition et à la sauvegarde d'une empreinte. Alternativement, l'information de mise en œuvre d'une sauvegarde biométrique peut être encodée dans la carte. Dans ce cas, afin d'éviter des cartes-clones qui se déclareraient systématiquement comme ne nécessitant pas de sauvegarde biométrique, un protocole cryptographique à base de signature numérique peut être mis en œuvre entre la carte et le terminal. Typiquement le TPE émettrait à l'intention de la carte un défi r et demanderait à la carte de lui retourner une signature numérique valable sur la chaîne (r | « pas de sauvegarde biométrique nécessaire »), où l'opérateur « | » désigne la concaténation. Les mises en œuvre de tels protocoles étant connue de l'homme de l'art.

D'une façon générale, la sauvegarde des données biométriques se fera, de préférence, en prenant la précaution d'en respecter la confidentialité.

Pour ce faire, une méthode particulièrement avantageuse consiste à chiffrer les données à bord du terminal à l'aide d'un algorithme de chiffrement probabiliste à clé publique dont seule la clé publique est contenue dans le terminal. Par exemple l'algorithme RSA OAEP. Ainsi, même en cas de violation du terminal les données biométriques restent confidentielles car le terminal ne contient aucun secret et peut seulement chiffrer l'information biométrique sans pour autant avoir la capacité de la déchiffrer. Plusieurs modes de réalisation sont possibles en ce qui concerne l'entité dont la clé publique sert à ce chiffrement. Cette entité peut être la banque de l'utilisateur, un tiers de confiance ou même l'utilisateur lui-même. Il va de soi que quelque en soit cette entité, sa clé publique doit dépendre d'une chaîne de certificats valables avant d'être acceptée par le TPE.

Par ailleurs, un TPE comprend généralement des moyens de saisie d'un code par un utilisateur (code utilisateur ou code PIN), ainsi que des moyens de validation de la saisie du code. Concrètement, les moyens de saisie d'un code comprennent un

clavier numérique ou alphanumérique et les moyens de validation de la saisie du code consistent généralement en une touche « validation » qui est destinée à être pressée par l'utilisateur une fois que celui-ci a saisi son code. La pression de cette touche indique au TPE que le code est saisi. Le TPE selon l'invention peut présenter de telles caractéristiques. Dans ce cas, les moyens d'acquisition de données biométriques sont distincts des moyens de saisie du code et des moyens de validation de la saisie du code. Le programme est alors adapté à enregistrer la saisie du code et à procéder à la validation du code par l'utilisateur puis à l'acquisition de données biométriques ou, inversement, à l'acquisition de données biométriques puis à la saisie du code et à la validation du code par l'utilisateur.

Mais selon un autre mode de réalisation, les moyens d'acquisition de données biométriques font office de moyens de validation de la saisie du code. Ainsi, le TPE ne comprend pas de touche « validation », celle-ci étant remplacée par les moyens d'acquisition de données biométriques. Le programme est alors configuré de telle sorte que l'utilisateur est appelé à saisir son code, puis à se prêter à l'acquisition de données biométriques, qui valide par ailleurs la saisie du code.

Un exemple de TPE se prêtant à l'implémentation de l'invention est maintenant décrit.

Ce TPE est doté d'un module de communication GSM/GPRS (bi-bande 900/1800 ou 900/1900 MHz). En cas d'incident sur le réseau GSM/GPRS, un modem optionnel peut, le cas échéant, assurer un fonctionnement continu.

Le TPE est par exemple équipé d'un processeur 32 bits prenant en charge les cryptographies usuelles (RSA, DES, triple DES...). L'architecture du processeur est de préférence choisie de sorte à permettre à plusieurs applications de fonctionner indépendamment les unes des autres (multi applicatif et multi tâches) au sein de l'appareil.

A cet égard, le programme décrit ci-dessus peut être chargé de manière indépendante des autres applications prévues dans le TPE, afin d'assurer une sécurité logique (ou étanchéité logicielle).

Une plateforme particulièrement adéquate pour mettre en œuvre l'invention est adaptée de la plateforme UNICAPT 32 d'Ingenico, construite autour d'un processeur 32 bits (module hardware HSC, pour "High Security Core") incluant une sécurité embarquée et un système d'exploitation multi applicatif supportant des langages de programmation avancés tels que C, C++ ou JAVA. Une telle plateforme s'intègre dans de nombreux environnements :

- Usage itinérant avec téléphonie mobile GPRS ou avec Bluetooth ;
- Environnements multi-caisses utilisant Ethernet ou Wi-Fi avec TCP/IP ;
- Commerçants à hauts volumes de vente utilisant ADSL ;

- Communication externe par USB/PCMCIA ;
- Connexion à Internet grâce à des points d'accès Wi-Fi.

Cette plateforme peut être modifiée (en particulier son programme de configuration) afin de permettre l'implémentation de caractéristiques selon l'invention.

L'invention n'est cependant pas limitée aux variantes décrites ci-avant mais est susceptible de nombreuses autres variations aisément accessibles à l'homme du métier. A titre d'exemple, il est possible de prévoir des applications de l'invention à des TPE fixes, portables et mobiles. De même, la description qui précède peut aussi se lire en remplaçant le TPE par un téléphone d'entreprise, un photocopieur d'entreprise ou tout dispositif où un contrôle de l'usage a posteriori serait de nature à dissuader la fraude, l'utilisation à contre-propos ou l'abus. Bien entendu, il convient de garder à l'esprit que le stockage des données biométriques dans le dispositif s'effectue, de préférence, indépendamment de la transaction (où de toute opération permise par ce dispositif, par exemple un appel téléphonique ou une photocopie) et qu'un contrôle des données biométriques stockées se fait, éventuellement, a posteriori. De la sorte, la confidentialité de ces données est préservée et ces données ne sont utilisées que sur requête spécifique, par exemple avec l'accord de l'utilisateur. Ici, l'abus ou la fraude sont découragé a posteriori. A titre d'exemple encore, on peut envisager un mode de réalisation dans lequel des données biométriques stockées dans une carte bancaire font office de données de référence ou données type. De plus, toute caractéristique physique telles que visage, voix, iris, rétine, pouce, forme de la main et de l'oreille, ADN peuvent faire l'objet de mesures biométriques aux fins d'application de l'invention. Par extension, on peut envisager d'utiliser des caractéristiques comportementales comme la signature ou la manière de taper sur un clavier.

REVENDICATIONS

1. Terminal de paiement électronique comprenant des moyens d'acquisition de données biométriques et un programme adapté à :
   - acquérir des données biométriques lors d'une transaction par l'intermédiaire des moyens d'acquisition de données biométriques ; et
   - stocker les données biométriques dans le terminal de paiement.

2. Terminal de paiement électronique selon la revendication 1, dans lequel le programme est en outre adapté à :
   - requérir auprès d'un central une autorisation de validation de la transaction ;
   - le cas échéant, recevoir du central l'autorisation de validation de la transaction et valider la transaction.

3. Terminal de paiement électronique selon la revendication 1 ou 2, dans lequel le programme est en outre adapté à :
   - stocker les données biométriques dans le terminal définitivement ou pendant une durée déterminée ;
   - fournir les données biométriques stockées, le cas échéant pendant la durée déterminée, et de préférence sous réserve que certaines conditions de sécurité soient satisfaites.

4. Terminal de paiement électronique selon la revendication 2, dans lequel le programme est en outre adapté à :
   - fournir les données biométriques au central avant de requérir l'autorisation de validation de la transaction ou simultanément.

5. Terminal de paiement électronique selon la revendication 2, dans lequel le programme est en outre adapté à :
   - recevoir du central des données biométriques de référence ;
   - établir une comparaison des données biométriques acquises aux données biométriques de référence ; et
   - valider ou non la transaction en fonction du résultat de la comparaison.

6. Terminal de paiement électronique selon l'une des revendications 1 à 5, dans lequel le programme est en outre adapté à :

- établir une comparaison des données biométriques avec des données type ; et
- le cas échéant, en fonction du résultat de la comparaison, ne pas valider la transaction ou acquérir de nouvelles données biométriques par l'intermédiaire des moyens d'acquisition de données biométriques.

7. Terminal de paiement électronique selon la revendication 5 ou 6, dans lequel le programme est en outre adapté à :

- établir la comparaison des données biométriques aux données biométriques de référence et / ou la comparaison des données biométriques aux données type par reconnaissance de forme.

8. Terminal de paiement électronique selon l'une des revendications 1 à 7, comprenant en outre des moyens de saisie d'un code par un utilisateur, et dont le programme est configuré de sorte que les moyens d'acquisition de données biométriques font office pour l'utilisateur de moyens de validation de la saisie du code.

9. Terminal de paiement électronique selon l'une des revendications 1 à 8, dans lequel les moyens d'acquisition de données biométriques sont choisis parmi les appareils photographiques permettant la capture d'images fixes ou mouvantes, les capteurs d'empreintes digitales, les capteurs de la forme de l'iris.

10. Terminal de paiement électronique selon l'une des revendications 1 à 9, dans lequel le programme est en outre adapté à chiffrer des données biométriques au sein du terminal à l'aide d'un algorithme de chiffrement probabiliste à clé publique, la clé publique appartenant à l'une des entités suivantes :

- La banque ;
- Le propriétaire de la carte ;
- Un tiers de confiance ; ou
- Le fabriquant du terminal.

11. Procédé de transaction comprenant :

- l'acquisition par un terminal de paiement électronique de données biométriques lors d'une transaction ; et
- le stockage des données biométriques dans le terminal de paiement.

12. Procédé selon la revendication 11, mis en œuvre avec le terminal de paiement électronique de l'une des revendications 1 à 10.

13. Procédé selon la revendication 11, comprenant en outre une étape de validation de la transaction indépendamment des données biométriques stockées.

RÉPUBLIQUE FRANÇAISE

2905187

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 682556
FR 0607440

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	US 6 957 770 B1 (ROBINSON TIMOTHY [US]) 25 octobre 2005 (2005-10-25) * abrégé * * colonne 5, ligne 9-55 * * colonne 6, ligne 11 - colonne 7, ligne 23 * * colonne 8, ligne 15-39 * * colonne 9, ligne 34-43 * * figures * -----	1-13	
X	US 6 980 670 B1 (HOFFMAN NED [US] ET AL) 27 décembre 2005 (2005-12-27) * abrégé * * colonne 7, ligne 17-44 * * colonne 17, ligne 64 - colonne 19, ligne 45 * * figures * -----	1-13	
X	EP 1 646 018 A (FUJITSU LTD [JP]; FUJITSU FRONTECH LTD [JP]) 12 avril 2006 (2006-04-12) * abrégé * * alinéas [0007] - [0009], [0018], [0033] - [0044] * * figures * -----	1-13	DOMAINES TECHNIQUES RECHERCHÉS (IPC) G06Q G06F
A	US 2004/258281 A1 (DELGROSSO DAVID [US] ET AL) 23 décembre 2004 (2004-12-23) * abrégé * * alinéas [0010], [0011] * * figures * -----	1-13	
A	WO 2005/098741 A (SOLIDUS NETWORKS INC [US]) 20 octobre 2005 (2005-10-20) * abrégé * * page 5, ligne 1 - page 7, ligne 16 * * page 12, ligne 4 - page 15, ligne 14 * * figures * -----	1-13	

Date d'achèvement de la recherche	Examinateur
14 mars 2007	Breugelmans, Jan

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0607440 FA 682556

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 14-03-2007
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 6957770 B1	25-10-2005	AUCUN	
US 6980670 B1	27-12-2005	AUCUN	
EP 1646018 A	12-04-2006	CN 1758266 A	12-04-2006
		JP 2006107398 A	20-04-2006
		KR 20060045644 A	17-05-2006
		US 2006080550 A1	13-04-2006
US 2004258281 A1	23-12-2004	AUCUN	
WO 2005098741 A	20-10-2005	CA 2562964 A1	20-10-2005
		EP 1743276 A2	17-01-2007

EPO FORM P0465