(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 021 799***

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

(21) **N° d'enregistrement national :** **14 54863**

(51) Int Cl[8] : ***G 07 C 9/00*** *(2013.01)*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 28.05.14.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 04.12.15 Bulletin 15/49.

(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 :**

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

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

(72) **Inventeur(s) :** LEGER MICHEL.

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

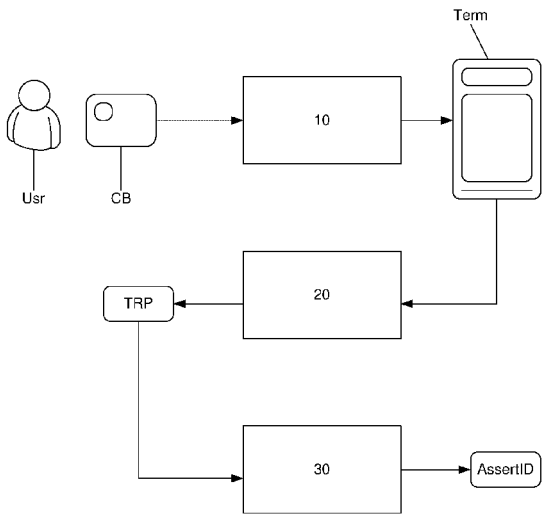
(74) **Mandataire(s) :** CABINET PATRICE VIDON.

(54) METHODE D'IDENTIFICATION, DISPOSITIF ET PROGRAMME CORRESPONDANT.

(57) L'invention se rapporte à un Procédé d'identification d'un utilisateur pour l'accès à un bien ou un service.

Selon l'invention, un tel procédé comprend:

- une étape de présentation à un terminal, par l'utilisateur à identifier, d'une carte de paiement;
- une étape d'exécution, par le terminal, d'une transaction de paiement dont le montant est nul;
- lorsque ladite transaction de paiement est exécutée sans erreur, une étape de délivrance d'une assertion d'identification entrainant l'accès au bien ou au service.



FR 3 021 799 - A1

Méthode d'identification, dispositif et programme correspondant

1. Domaine de l'invention

L'invention se rapporte au domaine de l'identification.

Plus particulièrement, l'invention se rapporte à l'identification d'individus par l'intermédiaire d'un élément d'identification. Un tel élément d'identification, dans le cadre de l'invention, s'entend comme une carte de paiement, une carte de crédit ou une carte de paiement. De telles cartes sont largement présentes et utilisées par de nombreuses personnes de part de monde afin de réaliser des opérations de paiement. Elles sont généralement distribuées par des établissements bancaires ou des prestataires de services de paiement. Une carte est généralement délivrée à un titulaire. Il s'agit en règle générale du client de la banque. Ce titulaire, client de la banque ou du prestataire de service de paiement, reçoit également un code d'identification personnel qu'il peut ou doit utiliser avec la carte de paiement (en fonction des contraintes d'autorisation et/ou du pays dans lequel la carte est utilisée). Ces cartes sont délivrées à l'issu d'un examen relativement minutieux de l'identité du demandeur (par exemple le client de la banque) : fourniture de pièce d'identité, de justificatifs de domicile, etc.

2. Art Antérieur

On fait la différence, dans la présente, entre les systèmes d'identification (pour obtenir une vérification d'identité) et les systèmes d'authentification (qui certifient l'identité). En effet, une vérification d'une identité ne met pas en œuvre les mêmes techniques qu'une authentification d'une identité : l'authentification est généralement forte alors que l'identification est comparativement relativement faible.

Il existe de nombreuses situations dans lesquelles il est nécessaire d'identifier une personne ou un individu. Une situation commune consiste par exemple à décliner son identité lorsque l'on se rend à un rendez-vous. En règle générale, le fait de décliner son identité n'est une preuve d'identité très forte et ce type d'identification n'est en pratique utilisé que dans des cas où l'identification ne revêt pas une importance très forte. Il en va différemment par exemple pour l'accès à un site protégé ou l'accès à des données sensibles. C'est par exemple le cas dans une entreprise. L'accès aux locaux d'une entreprise est en général limité à un nombre de personnes restreint. Ce sont par exemple les employés de l'entreprise et dans une moindre mesure aux clients et fournisseurs de l'entreprise. Souvent les employés sont identifiés à l'aide d'un badge qui sert de clés

d'accès aux locaux de l'entreprise. Les clients et fournisseurs, quant à eux, doivent se présenter à l'accueil de l'entreprise et fournir une pièce d'identité.

En tant que telle, la vérification de la pièce d'identité d'une personne ne peut être réalisée que par l'intermédiaire d'une personne physique, chargée de vérifier l'identité des personnes. Dans les situations où une personne physique n'est pas dédiée à la vérification de l'identité, des systèmes automatisés sont mis en œuvre (code d'accès à saisir sur un clavier, lecteurs de badges,...). Les systèmes d'identification automatisés sont nombreux et souvent chers.

Lorsqu'il s'agit de réaliser une authentification, des systèmes existent et sont encore plus chers. Ils mettent souvent en œuvre une reconnaissance biométrique (empreinte digitale par exemple). De tels systèmes sont réservés à un accès à des locaux extrêmement sensibles ou à des données ou des dispositifs du même type.

3. Résumé de l'invention

L'invention ne pose pas ces problèmes de l'art antérieur. Plus particulièrement l'invention offre une solution simple et peu couteuse pour permettre l'accès à des biens ou services tout en utilisant une architecture d'identification existante. L'invention se rapporte à un procédé d'identification d'un utilisateur pour l'accès à un bien ou un service. Selon l'invention un tel procédé comprend :

- une étape de présentation à un terminal, par l'utilisateur à identifier, d'une carte de paiement ;
- une étape d'exécution, par le terminal, d'une transaction de paiement dont le montant est nul ;
- lorsque ladite transaction de paiement est exécutée sans erreur, une étape de délivrance d'une assertion d'identification entrainant l'accès au bien ou au service.

Ainsi, la technique proposée permet d'autoriser un accès à un bien ou un service à partir d'une carte de paiement existante, appartenant à l'utilisateur. Cette technique évite de recourir à la fabrication de nouvelles cartes pour gérer ces accès.

Selon une caractéristique particulière, l'étape d'exécution d'une transaction de paiement de montant nul est adaptée, en types de contrôles réalisés conjointement entre la carte de paiement et le terminal, en fonction d'un degré de sensibilité d'accès.

Ainsi, l'application qui est implémentée au sein du terminal, qui est sensiblement identique à une application de paiement, est adaptée à la sensibilité des informations ou

des biens ou des services auxquels il est nécessaire d'accéder, et ce, sans qu'il soit nécessaire de prévoir une modification physique du terminal.

Selon un mode de réalisation particulier, l'étape d'exécution d'une transaction de paiement de montant nul comprend une étape de saisie, par ledit utilisateur, d'un code d'identification personnel sur un clavier du terminal.

Ainsi, l'utilisateur ne peut pas répudier son accès au bien ou au service : en effet, la saisie du code d'identification personnel apporte une quasi-certitude de l'identification de l'utilisateur.

Selon une caractéristique particulière, l'étape d'exécution d'une transaction de paiement de montant nul comprend une étape de transmission d'une requête d'autorisation à un serveur connecté audit terminal par l'intermédiaire d'un réseau de communication.

Ainsi, bien que d'un montant nul, cette transaction fait l'objet d'une acceptation en ligne par l'intermédiaire d'un serveur en charge, assurant de ce fait que la carte n'a pas été déclarée comme étant volée.

L'invention se rapporte également, dans au moins un mode de réalisation, à un dispositif d'identification d'un utilisateur pour l'accès à un bien ou un service. Selon une caractéristique particulière un tel dispositif comprend :

- des moyens de présentation, par l'utilisateur à identifier, d'une carte de paiement ;
- des moyens d'exécution, d'une transaction de paiement dont le montant est nul ;
- des moyens de délivrance d'une assertion d'identification entrainant l'accès au bien ou au service.

Un tel dispositif se présente bien entendu, dans sa forme la plus commune, comme un terminal. Un tel terminal tire avantage d'une infrastructure existante, qui est l'infrastructure formant le système interbancaire de paiement par carte. Le terminal peut avantageusement être connecté à un tel système afin de pouvoir mettre en œuvre au moins certaines des étapes du procédé proposé par ailleurs.

Selon une implémentation préférée, les différentes étapes des procédés selon l'invention 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 l'invention et étant conçu pour commander l'exécution des différentes étapes des procédés.

En conséquence, l'invention 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.

L'invention 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 l'invention 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, l'invention 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 l'invention.

4. Dessins

D'autres caractéristiques et avantages de l'invention 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 une architecture sur laquelle se base la technique proposée ;
- la figure 2 présente un synoptique de la technique proposée;
- la figure 3 décrit un dispositif de mise en œuvre de la technique proposée.

5. Description

5.1. Rappels

Le principe général de la technique proposée repose sur l'utilisation d'un terminal de paiement à des fins d'identification. Plus particulièrement, la technique proposée consiste à utiliser l'architecture générale du système de paiement par carte de paiement à des fins d'identification.

On décrit, en relation avec la figure 1, une architecture d'un système de paiement tel qu'implémenté à l'heure actuelle. Un tel système (S1) comprend au moins un terminal de paiement (POS) (un seul terminal représenté sur la figure), un serveur bancaire (BS)(ou un serveur de prestataire de services de paiements). Ce terminal de paiement (POS) et ce

serveur bancaire (BS) sont connectés d'une part par l'intermédiaire d'un réseau de communication (NTWK) (soit un réseau sans fils de type 3G, soit un réseau filaire) et éventuelle par un premier serveur intermédiaire (IS1).

En fonction des systèmes, le terminal de paiement n'est pas directement connecté au serveur bancaire. Il est par exemple connecté à un serveur intermédiaire, qui fait office de proxy/tampon/accréditeur (ce serveur intermédiaire peut être le serveur bancaire correspondant à la banque du commerçant). Le serveur intermédiaire (IS1) peut être lui-même connecté à au moins un autre serveur intermédiaire (IS2), qui est par exemple le serveur correspondant à l'organisme émetteur de la carte de paiement (Visa, Mastercard, American Express, etc.). Ce sont alors ces serveurs intermédiaires de seconde ligne qui sont connectés à des serveurs bancaires. Le serveur intermédiaire (IS1) peut être directement connecté aux autres serveurs bancaires (des autres banques et/ou fournisseurs de services de paiement).

Lorsqu'une transaction doit être réalisée à partir du terminal de paiement (POS), le terminal de paiement (POS) se connecte par exemple au premier serveur intermédiaire (IS1), notamment lorsqu'il est nécessaire de requérir une autorisation de paiement. En fonction du montant de la transaction, le serveur intermédiaire (IS1) peut fournir lui-même l'autorisation nécessaire ou requérir lune autorisation auprès d'un autre serveur. Le serveur intermédiaire (IS1) sélectionne, parmi l'ensemble des serveurs auquel il a accès (IS2, BS, etc.), le serveur idoine en fonction de la carte de paiement (CB) qui est présentée dans le terminal de paiement (POS) et requiert une autorisation auprès de ce serveur. Bien entendu, ces transmissions sont chiffrées à l'aide de matériels cryptographiques distribués entre les différents intervenants afin de garantir l'absence de fraudes et l'authenticité des informations échangées.

Par ailleurs, un ensemble de protocoles, appelés « EMV » est mis en œuvre afin d'obtenir, de la part de la carte de paiement, des données nécessaires à la transaction. La technique proposée se base sur cette architecture

La technique proposée, décrite en relation avec la figure 2, comprend les étapes suivantes :

- une étape de présentation (10) à un terminal (Term), par l'utilisateur à identifier (Usr), d'une carte de paiement (CB) ;

- une étape d'exécution (20), par le terminal (Term), d'une transaction de paiement (TrP) dont le montant est nul ;
- lorsque ladite transaction de paiement est exécutée sans erreur, une étape de délivrance (30) d'une assertion d'identification (AssertID) entrainant l'accès au bien ou au service.

La présentation de la carte de paiement peut consister en l'insertion de celle-ci dans un lecteur de carte de paiement ou encore en l'utilisation d'un mode de communication sans contact avec la carte de paiement (NFC) ou autre méthode de présentation d'une carte de paiement. Plus particulièrement, au moins deux modes de réalisation de la technique proposée peuvent être implémentés. Un premier mode de réalisation consiste à effectuer une identification d'un utilisateur en générant une transaction fictive avec un montant nul (0€). La mise en œuvre d'une telle transaction, qui est simple, permet de s'assurer que l'utilisateur de la carte de paiement, sur lequel est inscrit le nom du porteur est en possession de l'information relative au code d'identification personnel nécessaire à la validation de la transaction (lorsque le code d'identification personnel est utilisé). A priori donc, lorsque le code d'identification personnel est correct, l'utilisateur de la carte de paiement est supposé être la personne qu'il prétend.

Lorsqu'il n'est pas nécessaire de saisir le code d'identification personnel, seule la validité de la carte est assurée. Cette variante est particulièrement bien adaptée par exemple pour remplacer l'utilisation de cartes magnétiques, de cartes RFID ou de codes temporaires. En effet, par exemple pour accéder à une chambre d'hôtel, il est fréquent que celui-ci fournisse une carte magnétique au client. Cette carte est enfichée dans un lecteur présent sur la porte de la chambre et permet l'ouverture de celle-ci. À l'aide de la technique de l'invention, il n'est pas nécessaire d'utiliser une carte supplémentaire : la carte de paiement de l'utilisateur est utilisée en lieu et place de la carte magnétique pour permettre l'accès à la chambre. Lors de l'insertion de la carte, une transaction bancaire dont le montant est égal à zéro euro est construite par le lecteur de carte (par exemple intégrée à la porte de la chambre d'hôtel). Cette transaction est transmise soit au premier serveur intermédiaire soit au deuxième serveur intermédiaire. Celui-ci valide la transaction et transmet en retour une donnée représentative de la validation au terminal. Lorsque celui-ci reçoit la validation, il autorise l'action demandée (par exemple ouvrir la

porte). Alternativement, le terminal ne requiert aucune validation : une transaction avec un montant nul est construite. Lorsqu'il est possible de construire cette transaction (c'est à dire lorsque le terminal se trouve en présence d'une carte de paiement ou de crédit valide), alors le simple fait de pouvoir construire la transaction permet l'accès au produit ou au service souhaité. Bien entendu, en sus de la construction de cette transaction, le terminal vérifie que l'identifiant de la carte de paiement correspond à un identifiant attendu (l'identifiant étant par exemple le numéro de la carte de paiement). Si on se réfère à un accès à une chambre d'hôtel par exemple, on note que cet identifiant est nécessairement connu; en effet, pour pouvoir régler la chambre d'hôtel, l'utilisateur doit présenter une carte de paiement ou une carte de crédit valide à la réception de celui-ci : le numéro de la carte de paiement est donc déjà connu. Ainsi, dans ce mode de réalisation, on simplifie grandement le système de gestion de chambres de l'hôtel puisqu'il n'est pas nécessaire de disposer d'un système complémentaire d'éditions de carte magnétiques d'accès. Ce mode de réalisation est bien entendu dérivable à d'autres types d'accès à des biens ou des services.

Lorsqu'il est nécessaire de saisir le code d'identification personnel, une sécurisation supplémentaire est apportée par rapport aux systèmes existants : en effet, on vérifie alors que l'accès au bien ou au service n'est possible qu'au porteur de la carte qui dispose également du code d'identification personnel de cette carte. Ceci est intéressant dans le cas où l'accès au bien ou service doit être contrôlé de manière forte. Par exemple, ce type de fonctionnement peut être adapté à un dispositif de retrait de courrier en recommandé, qui peut être mis en place dans les postes. L'utilisateur qui reçoit un avis indiquant la disponibilité d'un courrier recommandé peut dès lors se rendre à la poste et utiliser un dispositif robotisé permettant de reconnaitre le porteur de carte de paiement, identifier le courrier recommandé en attente pour ce porteur, requérir, par l'intermédiaire du terminal, la saisie du code d'identification personnel et effectuer une transaction avec un montant nul. Lorsque le terminal reçoit l'autorisation du serveur, il donne l'ordre au dispositif robotisé de délivrer le courrier recommandé à l'utilisateur. Dès lors, il devient possible d'obtenir des biens et services de manière beaucoup plus sûre et rapide qu'auparavant. Plus particulièrement, la présente technique peut être mise en œuvre dans des situations d'accès à des biens et/ou services de manière non surveillée (en anglais "unatended"). Il s'agit de tout type de distributeur pour lequel une

identification ou une authentification d'un utilisateur (ou d'un client) est nécessaire, sans toutefois qu'une transaction financière soit nécessaire : accès à une place de parking, ouverture d'une porte, accès à un lieu de travail, etc.

Dans un autre mode de réalisation, complémentaire des modes de réalisation préalablement présentés, une transaction est réalisée avec chaque utilisation de la carte de paiement pour effectuer une opération d'identification. Comme explicité préalablement, dans un mode de réalisation de base, la transaction a un montant fixé à 0. De plus, dans ce mode de réalisation de base la transaction comprend également l'identité du "marchand", c'est à dire du fournisseur d'accès à la chose ou au service. Dans l'exemple de l'hôtel, il s'agit du nom de l'hôtel. La transaction comprend également un libellé, construit en fonction de l'action réalisée. Dans l'exemple de l'hôtel, il s'agit par exemple de l'heure d'utilisation.

Dans ce mode de réalisation, bien qu'il se présente comme un mode de réalisation de base, une subtilité est introduite au niveau de l'application qui gère les transactions d'identification/authentification (application installée au sein du terminal). On rappelle que le principe de l'invention consiste à utiliser une architecture d'un système général de paiement pour réaliser des identifications/authentifications. En fonction de la situation, et plus particulièrement en fonction de ce à quoi on souhaite offrir l'accès à l'aide de la carte de paiement, l'application installée au sein du terminal ne fonctionnera pas forcement de la même manière. Ainsi, dans le cas d'un accès « simple » la transaction peut être conduite sans nécessiter d'autorisation auprès d'un serveur (transaction hors ligne) : c'est par exemple le cas de l'accès à une chambre d'hôtel. Dans ce cas, la phase de gestion de risque du côté du terminal n'est pas mise en œuvre. Le bit idoine des « résultats de vérifications du terminal » du protocole EMV est positionné à 0.

Dans le cas d'un accès « sensible » (c'est-à-dire que les biens ou services auquel on souhaite accéder sont considérés comme sensible, comme par exemple le courrier en recommandé), la transaction est toujours conduite « en ligne », c'est-à-dire en requérant une autorisation auprès d'un serveur (par exemple un serveur bancaire). Dans ce cas, le bit 4 de l'octet 4 des « résultats de vérifications du terminal » du protocole EMV est positionné à 1, afin de forcer une transaction en ligne.

De manière corolaire, le fait de générer une transaction permet à l'utilisateur de disposer, sur son relevé de compte, de l'ensemble des utilisations de sa carte de

paiement, que ce soit pour réaliser un paiement ou pour obtenir un accès à un bien ou un service. Dès lors, le relevé de compte se transforme en un relevé d'actions.

Dans un mode de réalisation plus complexe, le terminal de paiement est utilisé non pas pour permettre un accès à un bien ou un service, mais pour réaliser une authentification d'une action du titulaire de la carte de paiement. Dans un tel mode de réalisation, la transaction réalisée par le terminal de paiement représente une chose identifiée. Il s'agit par exemple d'une donnée.

5.2. Autres caractéristiques et avantages

On décrit, en relation avec la figure 3, un dispositif mis en œuvre pour identifier un utilisateur, selon le procédé décrit préalablement.

Par exemple, le dispositif 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 un procédé d'identification.

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 une donnée d'activation (par exemple un appui sur un bouton ou une commande d'activation numérique). Le microprocesseur de l'unité de traitement 32 met en œuvre les étapes du procédé d'identification, selon les instructions du programme d'ordinateur 33 pour requérir la présentation d'une carte de paiement (soit par insertion dans un lecteur de cartes, soit par transmission sans contact), pour effectuer une transaction financière d'un montant nul et pour délivrer une assertion d'identification lorsque cette transaction est exécutée correctement.

Pour cela, le dispositif comprend, outre la mémoire tampon 31, des moyens de communications, tels que des modules de communication réseau, des moyens de transmission de donnée et un processeur de chiffrement.

Ces moyens peuvent se présenter sous la forme d'un processeur particulier implémenté au sein du dispositif, ledit processeur étant un processeur sécurisé. Selon un mode de réalisation particulier, ce dispositif met en œuvre une application particulière qui est en charge de la réalisation des transactions, cette application étant par exemple fournie par le fabricant du processeur en question afin de permettre l'utilisation dudit

processeur. Pour ce faire, le processeur comprend des moyens d'identification uniques. Ces moyens d'identification uniques permettent d'assurer l'authenticité du processeur.

Par ailleurs, le dispositif comprend en outre les moyens d'autorisation d'accès à un bien ou un service comme des moyens de déclenchement d'ouverture (portes par exemple). Ces différents moyens se présentent également comme des interfaces de communications permettant d'échanger des données sur des réseaux de communication, des moyens d'interrogations et de mise à jour de base de données, ...

Revendications

1. Procédé d'identification d'un utilisateur pour l'accès à un bien ou un service, procédé caractérisé en ce qu'il comprend :
   - une étape de présentation à un terminal, par l'utilisateur à identifier, d'une carte de paiement ;
   - une étape d'exécution, par le terminal, d'une transaction de paiement dont le montant est nul ;
   - lorsque ladite transaction de paiement est exécutée sans erreur, une étape de délivrance d'une assertion d'identification entrainant l'accès au bien ou au service.

2. Procédé d'identification selon la revendication 1, caractérisé en ce que l'étape d'exécution d'une transaction de paiement de montant nul est adaptée, en types de contrôles réalisés conjointement entre la carte de paiement et le terminal, en fonction d'un degré de sensibilité d'accès.

3. Procédé d'identification selon la revendication 1, caractérisé en ce que l'étape d'exécution d'une transaction de paiement de montant nul comprend une étape de saisie, par ledit utilisateur, d'un code d'identification personnel sur un clavier du terminal.

4. Procédé d'identification selon la revendication 1, caractérisé en ce que l'étape d'exécution d'une transaction de paiement de montant nul comprend une étape de transmission d'une requête d'autorisation à un serveur connecté audit terminal par l'intermédiaire d'un réseau de communication.

5. Dispositif d'identification d'un utilisateur pour l'accès à un bien ou un service, dispositif caractérisé en ce qu'il comprend :
   - des moyens de présentation, par l'utilisateur à identifier, d'une carte de paiement ;
   - des moyens d'exécution, d'une transaction de paiement dont le montant est nul ;

- des moyens de délivrance d'une assertion d'identification entrainant l'accès au bien ou au service.

6. 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 d'identification selon la revendication 1, lorsqu'il est exécuté sur un ordinateur.

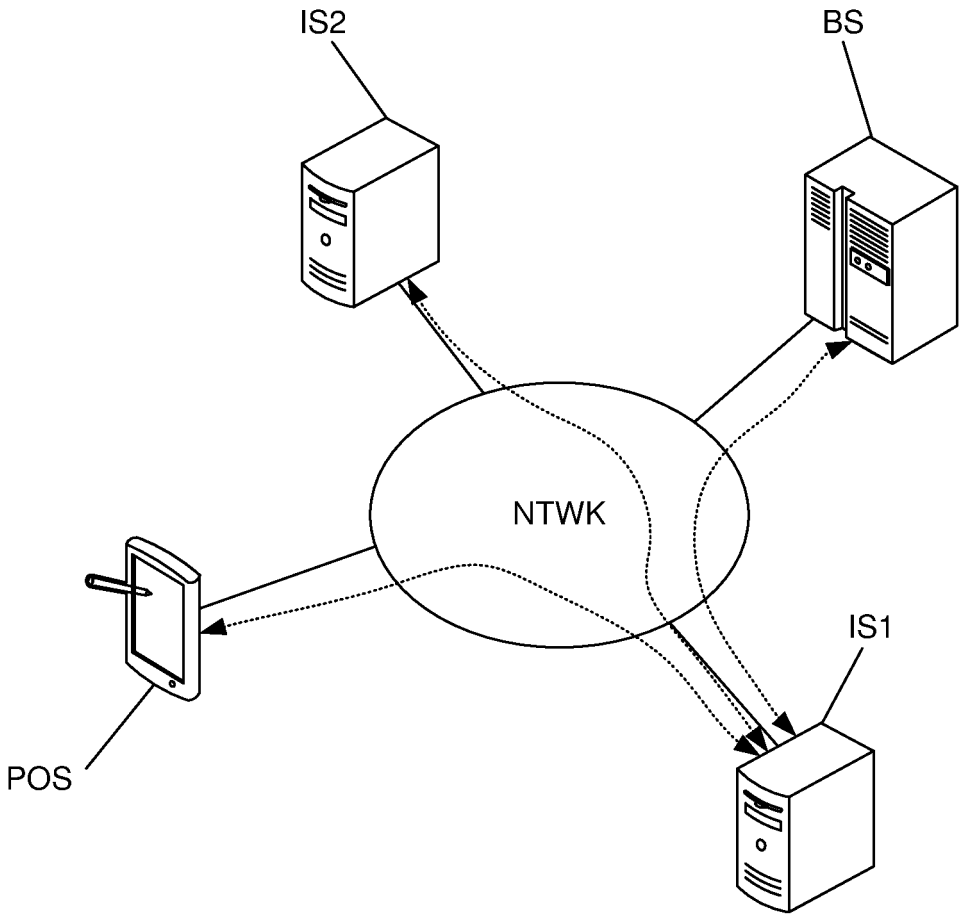


Figure 1

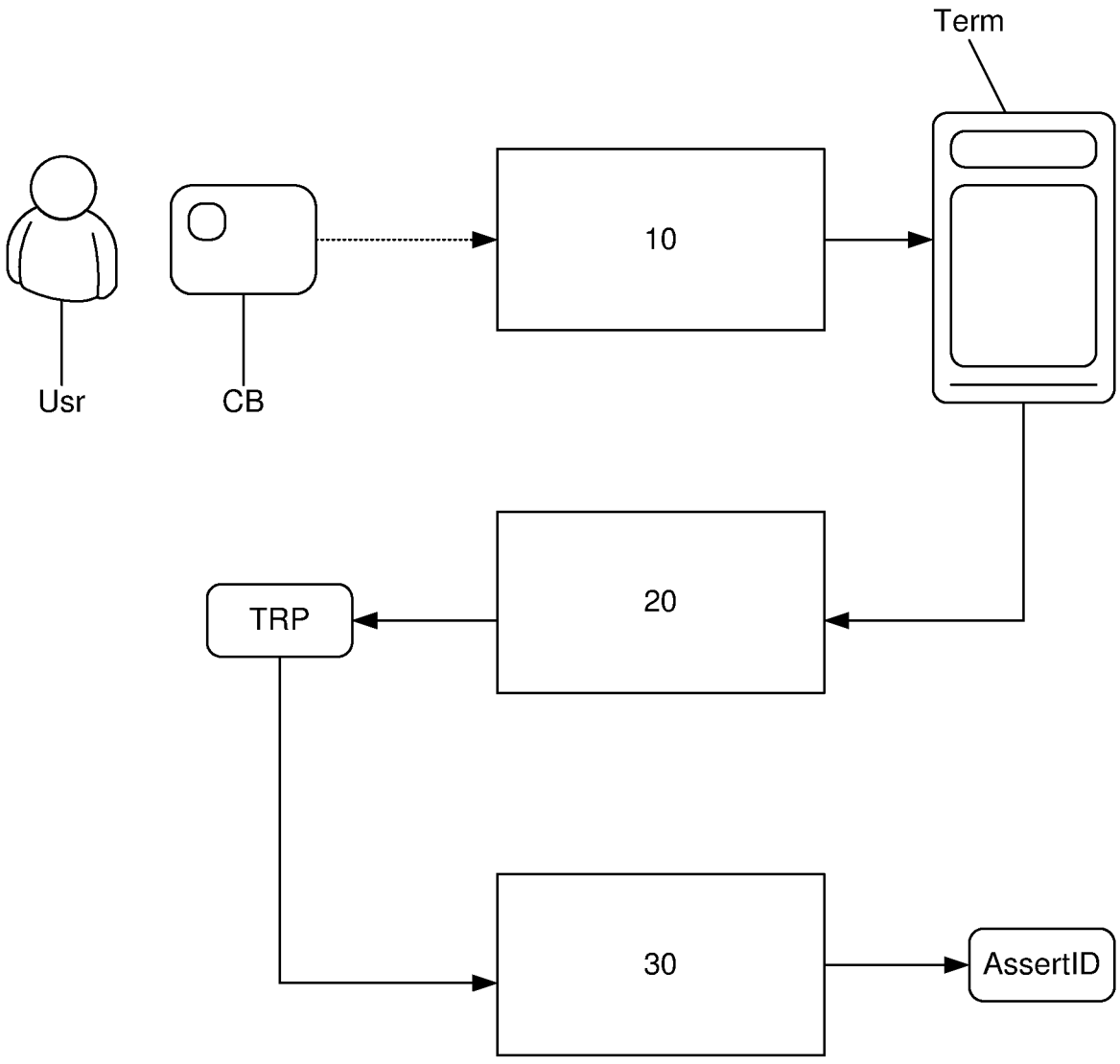


Figure 2

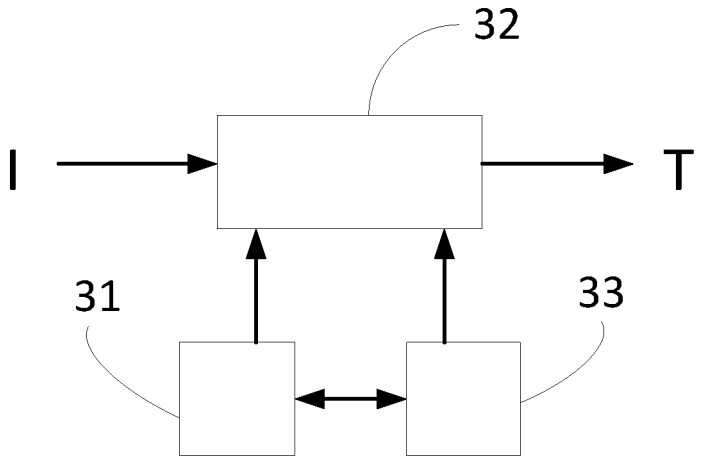


Figure 3

RÉPUBLIQUE FRANÇAISE

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 795521
FR 1454863

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 2012/143768 A1 (HAMMAD AYMAN [US] ET AL) 7 juin 2012 (2012-06-07) * alinéa [0045] - alinéa [0052] * * alinéa [0107] - alinéa [0113] * * figures 9,10 * * alinéa [0036] - alinéa [0037] * * alinéa [0059] - alinéa [0063] *	1-6	G07C9/00
X	US 2001/034723 A1 (SUBRAMANIAM ARUN K [US]) 25 octobre 2001 (2001-10-25) * alinéa [0022] - alinéa [0039] * * figures 1,2 *	1,3-6	
E	WO 2014/093390 A1 (VISA INT SERVICE ASS [US]) 19 juin 2014 (2014-06-19) * alinéa [0009] - alinéa [0010] * * alinéa [0026] - alinéa [0033] * * alinéa [0047] - alinéa [0060] * * alinéa [0146] - alinéa [0182]; figures *	1,3-6	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC) G07C G06Q

Date d'achèvement de la recherche	Examinateur
10 février 2015	Miltgen, Eric

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 1454863 FA 795521

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 10-02-2015
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 2012143768 A1	07-06-2012	US 2012136796 A1	31-05-2012
		US 2012143768 A1	07-06-2012
		WO 2012040377 A1	29-03-2012
US 2001034723 A1	25-10-2001	AU 3686401 A	20-08-2001
		US 2001034723 A1	25-10-2001
		WO 0159545 A2	16-08-2001
WO 2014093390 A1	19-06-2014	US 2014164254 A1	12-06-2014
		WO 2014093390 A1	19-06-2014

EPO FORM P0465