(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 808 144**

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

(21) **N° d'enregistrement national :** **00 05109**

(51) Int Cl[7] : **H 04 L 9/00,** G 06 F 17/60

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 20.04.00.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 26.10.01 Bulletin 01/43.

(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) :** *BOURDIN MICHEL PAUL* — FR.

(72) **Inventeur(s) :** BOURDIN MICHEL PAUL.

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

(74) **Mandataire(s) :** CABINET DE BOISSE ET COLAS.

(54) PROCEDE ET SYSTEME DE PAIEMENT ELECTRONIQUE.

(57) Ce procédé de paiement électronique comprend les étapes de:

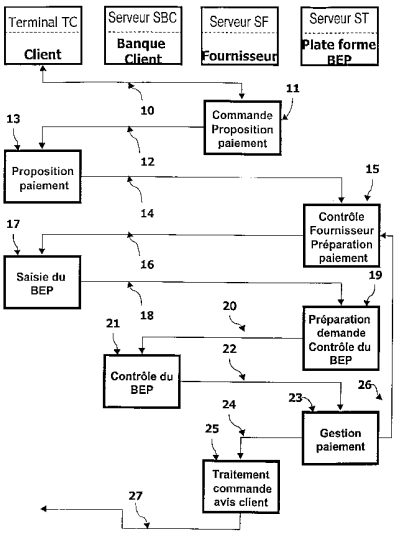
a) génération conditionnelle par un établissement financier, en réponse à une requête dudit client, d'un code unique et non prédictible représentatif d'un bon de paiement (BEP) de valeur maximale prédéterminée,

b) transmission dudit code audit client,

c) stockage par ledit établissement financier dans un serveur de paiement (SBC) de données représentatives dudit bon, lesdites données représentatives comprenant au moins ledit code, ladite valeur et des données d'identification dudit client,

d) transmission par ledit client, à un serveur (ST) de traitement de bon électronique, de données de paiement comprenant ledit code et une somme déterminée, en réponse à une demande de paiement de ladite somme émanant d'un fournisseur (SF), et

e) validation conditionnelle, par ledit serveur de paiement (SBC), du paiement de ladite somme audit fournisseur en réponse à la transmission électronique par ledit serveur de traitement (ST) d'une demande de validation dudit bon.



FR 2 808 144 - A1

La présente invention concerne un procédé et un système de paiement électronique en ligne sur un réseau de communication tel que le réseau Internet.

On connaît des instruments de paiement utilisables dans le cadre de l'Internet : le chèque, les cartes de paiement, le porte-monnaie électronique.

Le chèque répond mal au contexte de l'Internet, tant par ses délais d'acheminement que ses coûts de "compensation" en cas de paiement International.

Les porte-monnaie électroniques sont principalement destinés à des paiements de petit montant. Ils doivent être rechargés ce qui immobilise des fonds inactifs pour le porteur, et leur acceptation n'est pas généralisée.

Les cartes de paiement sont bien adaptées au contexte de l'Internet, par leur acceptation universelle, par leur traitement électronique, et parce qu'elles permettent des transactions de montant élevé. Toutefois, elles présentent l'inconvénient de reposer sur un numéro de carte qui est en quelque sorte une clé d'accès à un compte. Elles demandent donc la mise en œuvre de fonctions d'identification et d'authentification du client afin de s'assurer qu'il est bien le titulaire de la carte dont il présente les références. Elles demandent également que ce numèro de carte, référence sensible, soit fortement protégé au cours de sa transmission sur le réseau afin de ne pouvoir être intercepté et utilisé par un tiers malveillant. Des protocoles d'échange sécurisés ont été développés (SSL ; SET). Leur mise en œuvre est toutefois complexe (elle demande des certificats numériques d'identité), lourde en bande passante, et requiert l'inter-opérabilité des moyens cryptographiques utilisés. De plus la sécurisation apportée ne concerne que la fonction d'échange, mais ces numéros, une fois transmis doivent être stockés dans des systèmes d'information qui deviennent eux la cible des pirates.

C'est ainsi qu'a déjà eu lieu un chantage auprès d'un site Internet sur lequel 300.000 numéros de carte avaient été détournés. Le voleur menaçait ce site de divulguer ces numéros de carte, ce qui portait atteinte à la confiance de ses clients.

De façon beaucoup plus simple, ces numéros de carte sont imprimés sur les facturettes de paiement non protégées (elles restent parfois au fond

des caddies de supermarchés ou sur des distributeurs de billets) que des petits voleurs peuvent ainsi très simplement se procurer.

On ne saurait omettre également qu'il existe, sur Internet, des logiciels capables de produire des faux numéros de cartes bancaires qui sont acceptés par les systèmes de paiement. Ainsi, une fraude massive (10% des paiements) a déjà pu se développer pour le rechargement de téléphones mobiles, en utilisant des références de cartes obtenues par ces procédés.

En conclusion, malgré son adaptation au contexte électronique, la carte présente une faiblesse majeure, celle d'un identifiant, dont la protection reste complexe et aléatoire, qui de plus permet de suivre la trace de l'activité d'un utilisateur sur l'Internet.

L'invention vise à fournir un procédé et un système qui permettent d'assurer de manière simple et sûre des paiements électroniques en ligne, notamment via Internet, tout en limitant le risque financier encouru par l'auteur du paiement dans l'éventualité improbable d'une fraude.

Un autre but de l'invention est de fournir un procédé et un système de paiement électronique sécurisé susceptible de bénéficier de la confiance d'utilisateurs déstabilisés par les incidents auxquels sont sujets les moyens de paiement conventionnels.

L'invention vise également à fournir un procédé et un système de paiement électronique sécurisé qui puissent aisément être mis en oeuvre par tous les acteurs concernés par de tels paiements (banques, commerçants, clients, ...), indépendamment de la nature de leur activité, de leur localisation géographique, etc.

A cet effet, l'invention a pour objet un procédé de paiement électronique d'un fournisseur par un client via un réseau de communication, caractérisé en ce qu'il comprend les étapes de :

a) génération conditionnelle par un établissement financier, en réponse à une requête dudit client, d'un code unique et non prédictible représentatif d'un bon de paiement de valeur maximale prédéterminée,

b) transmission dudit code audit client,

c) stockage par ledit établissement financier dans un serveur de paiement de données représentatives dudit bon, lesdites données représentatives comprenant au moins ledit code, ladite valeur et des données d'identification dudit client,

d) transmission par ledit client, à un serveur de traitement de bon électronique, de données de paiement comprenant ledit code et une somme déterminée, en réponse à une demande de paiement de ladite somme émanant d'un fournisseur, et,

e) validation conditionnelle, par ledit serveur de paiement, du paiement de ladite somme audit fournisseur en réponse à la transmission électronique par ledit serveur de traitement d'une demande de validation dudit bon.

Ainsi, aucune "clé de compte" ne circule sur le réseau. La confidentialité nécessaire lors des échanges entre le client et le fournisseur est allégée puisque le besoin est réduit à la résistance de quelques secondes à une attaque : le délai entre l'envoi du bon électronique de paiement par le client et sa présentation à l'établissement financier.

Selon une caractéristique de l'invention, lesdites données de paiement comprennent des données d'identification dudit fournisseur, ledit code et ladite somme, et ledit serveur de traitement :

* contrôle l'identité dudit fournisseur en réponse à la réception desdites données de paiement,
* transmet conditionnellement ladite demande de validation audit serveur de paiement, en fonction du résultat dudit contrôle, et
* transmet électroniquement audit fournisseur une information de validation de paiement de ladite somme en réponse à ladite validation dudit bon par ledit serveur de paiement.

De préférence, ladite étape d) comprend :

d1) la transmission électronique, dudit fournisseur audit client, d'une facture électronique comprenant ladite somme et des premières données d'identification dudit fournisseur et de ladite facture,

d2) la transmission électronique de ladite facture dudit client audit serveur de traitement en réponse au choix par ledit client de son règlement par un bon de paiement électronique,

d3) le contrôle de l'identité dudit fournisseur par ledit serveur de traitement au moyen desdites premières données d'identification en réponse à la réception de ladite facture,

d4) la construction et la transmission électronique audit client, par ledit serveur de traitement, d'un formulaire de paiement en réponse à la validation dudit contrôle de l'identité dudit fournisseur, ledit formulaire de paiement comprenant ladite somme et des secondes données d'identification dudit fournisseur et de ladite facture, et

d5) l'introduction dudit code dans ledit formulaire par ledit client pour constituer un message de paiement,

ledit serveur de traitement transmettant ladite demande de validation audit serveur de paiement en réponse à la réception dudit message de paiement.

Selon une autre caractéristique de l'invention, ladite étape e) comprend la mise en oeuvre par ledit serveur de paiement des opérations de :

e1) comparaison du code reçu dudit client via ledit serveur de traitement avec ledit code stocké à l'étape c),

e2) vérification que le bon représenté par ledit code stocké n'a pas été utilisé antérieurement, et

e3) comparaison de ladite somme à ladite valeur stockée à l'étape c).

Selon une autre caractéristique de l'invention,

- lesdites étape a) et c) comprennent l'attribution et le stockage par et dans ledit serveur de paiement d'au moins une condition limitative relative au contexte d'utilisation dudit bon, et
- ladite étape e) comprend la vérification par ledit serveur de paiement du respect par ladite demande de validation de ladite condition limitative attribuée audit bon.

Selon une autre caractéristique de l'invention, ladite condition limitative appartient au groupe comprenant :

- une date de péremption dudit bon,

- une limitation de l'utilisation dudit bon dans le cadre d'une catégorie d'activité déterminée,
- une limitation de l'utilisation dudit bon pour le paiement d'au moins un fournisseur déterminé,
- l'association audit message transmis audit serveur de traitement d'une signature électronique dudit client.

De préférence, ladite demande de validation comprend des données de datation générées par ledit serveur de traitement pour le contrôle par ledit serveur de paiement de la date de péremption dudit bon.

Selon une autre caractéristique de l'invention, lesdites étapes a), b) et d) comprennent :

- la transmission électronique par ledit client, à partir d'un terminal, de ladite requête audit serveur de paiement,
- la transmission électronique par ledit serveur de paiement dudit code audit terminal,
- la transmission électronique desdites données de paiement audit serveur de traitement à partir dudit terminal.

De préférence, ladite transmission électronique est effectuée via un canal de communication sécurisé.

L'invention a également pour objet un système de paiement électronique pour la mise en oeuvre du procédé défini ci-dessus, caractérisé en ce qu'il comprend

- au moins un terminal d'accès d'au moins un client à une application de paiement électronique et à un réseau de communication,
- au moins un serveur de paiement connecté audit réseau de communication et comprenant :
  * des moyens de génération conditionnelle dudit code pour la mise en oeuvre de ladite application,
  * des moyens de stockage desdites données représentatives dudit bon, et
  * des moyens de transmission dudit code audit terminal,
- au moins un serveur fournisseur connecté audit réseau de communication et comprenant des moyens d'élaboration et de

transmission audit terminal, dans le cadre de ladite application, d'une facture susceptible d'être payée au moyen dudit bon, et

- au moins un serveur intermédiaire de traitement de bons électroniques comprenant :
  * des moyens de construction d'un message de demande de validation dudit bon en réponse à la réception d'un message de paiement émanant dudit client,
  * des moyens de transmission dudit message de demande de validation audit serveur de paiement, et
  * des moyen de transmission audit serveur fournisseur d'une information de validation de paiement en réponse à la validation dudit bon par ledit serveur de paiement.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description qui suit d'un mode de réalisation particulier non limitatif de l'invention illustré par les dessins annexés sur lesquels:

- la figure 1 est un schéma illustrant les organes essentiels d'un système pour la mise en oeuvre du procédé de paiement électronique selon l'invention,

- la figure 2 est un schéma synoptique illustrant le processus d'obtention d'un bon électronique de paiement du procédé selon l'invention,

- la figure 3 est un schéma synoptique illustrant le processus de paiement au moyen du bon électronique de paiement, et

- la figure 4 est un schéma synoptique illustrant le traitement d'un bon électronique de paiement postérieurement au paiement proprement dit.

En se reportant à la figure 1, un système pour la mise en oeuvre du procédé électronique de paiement qui sera décrit dans la suite comprend les organes essentiels suivants, susceptibles de communiquer entre eux par l'intermédiaire d'un réseau de communication R tel que le réseau Internet :

- des terminaux clients TC, tels que des ordinateurs personnels, assistants personnels (PDA), téléphones portables ou autres, permettant à des clients d'accéder au réseau R et comportant la partie "client" des logiciels d'application nécessaires pour la mise en oeuvre des fonctionnalités de paiement électronique qui seront

décrites dans la suite. Pour la simplicité du dessin, un seul terminal TC a été représenté à la figure 1 ;

- un serveur SBC d'une banque ou établissement financier, ci-après appelé serveur de paiement, qui assure à la fois les fonctions de banque à domicile pour l'attribution de bons électroniques de paiement à ses clients dotés d'un terminal TC et de serveur de paiement dans le cadre de la négociation d'un bon électronique de paiement décrite ci-après. Il existe, bien entendu, autant de serveurs SBC qu'il y a de banques participant au système de paiement électronique. En variante, les fonctions remplies par le serveur SBC peuvent être réparties entre plusieurs serveurs, étant entendu que le ou les serveurs assurant les fonctions de paiement proprement dit peuvent accéder aux informations relatives à des bons de paiement électroniques attribués par le ou les serveurs assurant la fonction de banque à domicile ;
- un ou plusieurs serveurs commerçants ou fournisseurs SF auxquels des clients peuvent accéder pour passer des commandes en ligne à partir de leurs terminaux TC et qui sont susceptibles de transmettre à ces derniers des factures électroniques via le réseau R ;
- un serveur bancaire SBF d'une banque ou établissement financier chez qui un commerçant ou fournisseur ayant un serveur SF dispose d'un compte qui se verra crédité à l'issue d'une transaction avec un client se soldant par un paiement effectué au moyen d'un bon de paiement électronique. Bien entendu, le nombre de serveur bancaires SBF n'est pas limité ;
- un serveur ST de traitement de bons électroniques, ou plate-forme BEP, jouant un rôle d'intermédiaire ou de médiation entre les différentes entités décrites ci-dessus et faisant office de pare-feu et de tiers de confiance vis-à-vis de celles-ci. En variante, il peut être bien entendu prévu plusieurs serveurs de traitement ST.

Le processus complet de mise en œuvre du procédé de paiement électronique selon l'invention peut être décomposé en trois grandes étapes :

l'obtention d'un bon électronique de paiement, la négociation d'un bon électronique de paiement, le post traitement d'un bon électronique de paiement.

La figure 2 présente la première étape du procédé: l'obtention d'un bon électronique de paiement, ci-après également appelé BEP. On suppose qu'au préalable, le client a conclu avec sa banque un accord d'utilisation de ce moyen de paiement.

Le client se connecte par son terminal TC au serveur SBC de sa banque et établit avec celui-ci une session sécurisée qui garantit l'intégrité et la confidentialité des échanges. Après une série d'échanges 1 qui aboutit de la part du client à une demande de BEP, la banque (serveur SBC) construit le formulaire " demande de BEP " 2 et le lui adresse en 3. Ce formulaire permet en 4 au client de fixer le montant demandé et de choisir éventuellement parmi différentes options offertes : utilisation du BEP limité à un type d'activité, à des paiements d'un ou plusieurs fournisseur déterminés, contre-signature par exemple. Il signe alors électroniquement sa demande ou requête avant de la retourner en 5 à sa banque. La signature électronique de la demande ou requête lui confère une valeur contractuelle dans les pays, de plus en plus nombreux, qui reconnaissent légalement la signature électronique.

A réception de la demande complétée et signée, la banque client (serveur SBC) construit en 6 un code ou référence de BEP, qui contient au moins les données d'identification de la banque client dans le système BEP (afin que la plate-forme de paiement ST identifie l'émetteur d'un BEP lors de sa présentation), et un numéro unique et non prédictible, c'est-à-dire construit de manière à ce que sa connaissance ne permette pas de déduire un autre code.

Un procédé, non limitatif, permettant de construire un tel numéro unique, est de chiffrer un compteur, incrémenté à chaque demande d'une valeur connue de la banque client, par un mécanisme cryptographique à clé secrète connue seulement de la banque client. Par ce procédé, seule la banque client connaissant la valeur qui est chiffrée et la clé utilisée pour le chiffrement, toute attaque cryptographique, et par là même, toute tentative de construire un code de BEP valide pour un fraudeur est impossible. Il faudrait

en effet que le code recalculé par la banque réceptrice corresponde à un code de BEP qu'elle a émis et cette probabilité est inférieure à 10^{-10} avec une clé de 8 caractères en admettant que la banque gère un portefeuille de 1.000.000.000 de BEP actifs. On peut encore accroître la difficulté en publiant une partie de la valeur chiffrée : le défi devient alors non seulement de fournir une valeur existante, mais également une partie de sa traduction. Ainsi avec 3 caractères " de contrôle " la probabilité passe à 10^{-13}. (environ 1.000.000 de fois moins que de gagner au loto !). Enfin, la limitation de la valeur d'un bon électronique de paiement (BEP) à une valeur imprévisible réduit l'intérêt d'une attaque car la probabilité :

1) de trouver un numéro par hasard,
2) d'en trouver la traduction par hasard et
3) que le montant associé soit significatif,

est encore plus faible.

Après génération d'un code de BEP en 8, la banque client (serveur SBC) enregistre sa " racine " (la valeur qui a été chiffrée pour le calculer) dans son système de stockage d'informations, avec le compte client associé, ses paramètres, sa date de création. Cette dernière permettra de déterminer la date de péremption du BEP en fonction de la durée de validité assignée par la banque émettrice au BEP. L'enregistrement de la " racine " du code de BEP protège la banque de toute attaque sur son système de stockage d'informations, puisque c'est le code chiffré qu'il faut produire au commerçant : accéder à la racine ne permet pas de connaître un code de BEP.

En 7, le code de BEP est retourné au client en réponse à sa demande (sous protocole sécurisé, pour en garantir la confidentialité) . Il est accompagné de ses caractéristiques (montant, cadre d'utilisation) qui peuvent être utiles au client au moment du paiement pour choisir le BEP adapté à sa transaction. Le client est alors responsable de la sécurité de son code de BEP, (comme il est responsable des billets qu'il retire de sa banque), et le stocke sur le support de son choix en 9. Il est possible au client de consulter sur son terminal TC la liste de ses BEP actifs à tout moment, à travers ses outils de banque à domicile, ou directement dans un dossier BEP qu'il aurait

lui même constitué. Le client a la faculté de transmettre un BEP à un tiers, comme un billet de banque, en lui communiquant le code de ce BEP.

Il est important de noter que dans ce processus, le compte du client n'a pas été débité, c'est-à-dire que la requête ou demande d'un BEP n'immobilise pas de capitaux non productifs. Il faut également noter que la perte du BEP est sans conséquences financières pour le client : le BEP non utilisé s'annulera de lui même à sa date de péremption.

La figure 3 illustre la deuxième étape du processus : le paiement.

Le client se connecte par son terminal TC sur un site marchand (serveur SBC) et, par une série d'échanges 10, passe sa commande. A la fin des échanges, sur demande du client, le serveur SF construit une facture 11 et l'adresse en 12 au client. Cette facture contient au moins les données d'identification du fournisseur ou commerçant dans le serveur ST, le montant de la facture, une référence de facture. Elle contient également des propositions de modes de règlement, dont le BEP. Le code de BEP détenu par le client correspond à un lien vers le serveur ST (plate-forme BEP). Pour pouvoir proposer un paiement par BEP, le commerçant doit avoir obtenu l'agrément de sa banque SBF qui doit elle-même être participante à ce système de paiement. L'agrément du commerçant par une banque constitue une " labellisation " qui est elle-même un élément de confiance.

Le choix en 13, par le client, du règlement au moyen d'un bon électronique de paiement, le met automatiquement (hyperlien) en relation en 14 avec le serveur ST auquel il transmet les éléments de la facture contenant notamment le numéro du commerçant, ainsi que le montant et la référence de la facture. Le serveur ST peut alors contrôler que le commerçant est référencé dans la plate-forme BEP et construire en 15 un formulaire de paiement. Ce formulaire, destiné à la saisie du code de BEP, est adressé au Client en 16 dans une session sécurisée qui garantit la confidentialité des échanges. Le formulaire reçu en 17 par le client sur le terminal TC reprend le montant de la facture, le numéro et les données d'identification du commerçant et une date/heure fournie par le serveur ST. Le client choisit un BEP adapté au paiement et en saisit le code sur le formulaire 17 avant de

l'adresser en 18, dans une session sécurisée, au serveur ST (plate-forme BEP).

Il est important de noter à ce niveau que ce processus ne comporte aucune fonction d'identification du client par le serveur ST, et que le client n'a pas besoin d'être équipé d'un lecteur de carte affichant le montant de la transaction pour éviter une fraude basée sur une différence entre la valeur affichée à l'écran et la valeur " signée " par le client. Le client est protégé par la valeur du BEP qu'il transmet et qui limite implicitement le montant maximal débitable (qui n'est connu que de lui-même et de sa banque) : toute tentative de majoration risque de conduire à un dépassement de la valeur du BEP et donc à son rejet.

Avant de renvoyer le BEP au serveur ST, le client a la possibilité de le contresigner électroniquement avec la facture. La signature inclut le montant, le code de BEP, le numéro de facture, le numéro du commerçant et la date de la transaction. Cette contre signature permet à sa banque (serveur SBC) d'authentifier son client si celui-ci le souhaite.

A réception du BEP, le serveur ST construit en 19 un message de demande de validation ou vérification destiné à être adressé au serveur SBC (banque client). Ce message contient le montant de la facture, le code de BEP, mais également les informations sur le commerçant qui peuvent être nécessaires à la validation du paiement : catégorie de commerçant et numéro de commerçant. Ce message est adressé en 20 au serveur SBC (banque client) par une liaison sécurisée.

A réception de la demande de paiement, le serveur SBC contrôle en 21 la compatibilité du BEP qui lui est présenté avec le paiement demandé : vérification que le BEP a bien été émis par la banque client, qu'il n'a pas déjà été utilisé, qu'il n'est pas périmé, que sa valeur est supérieure ou égale au montant de la transaction, qu'il est contresigné si son client a choisi cette option, que le commerçant satisfait aux conditions limitatives éventuelles (Catégorie d'activité, identité du commerçant), enfin que le compte présente une provision suffisante. Si l'ensemble des conditions est satisfait, le serveur SBC débite immédiatement le compte du client du montant de la facture (comme dans le cas d'un retrait à un distributeur). Il avise alors en 22 la plate-

forme BEP (serveur ST) de son accord ou de son refus de paiement. Dans le cas d'un refus, le serveur de banque client SBC ne fournit aucune indication sur les raisons de ce refus pour des raisons de sécurité. Dans tous les cas, le BEP présenté devient inutilisable pour un nouveau paiement.

Il faut noter que, dans le mode de réalisation décrit, la négociation d'un BEP implique obligatoirement l'intermédiation de la plate-forme BEP (serveur ST). Cette obligation protège la banque client (serveur SBC) d'une attaque par des commerçants qui utiliseraient des codes BEP aléatoires. La plate-forme BEP (serveur ST) joue en quelque sorte un rôle de pare-feu vis-à-vis de la banque client (serveur SBC).

A réception de la réponse, le serveur ST enregistre en 23 la transaction s'il y a accord de la banque client, sinon elle revient en 26 à l'envoi au client d'un formulaire de saisie de BEP (une erreur de saisie du code de BEP peut être à l'origine du rejet). Toutefois cette offre de correction n'est proposée qu'un nombre limité de fois pour une même référence ou numéro de facture afin d'interdire à un client fraudeur, ou à un automate de fraude, d'essayer des codes de BEP aléatoires.

Le serveur ST avise alors en 24 le commerçant du succès ou de l'échec du paiement.

Selon la réponse, le commerçant engage ou non en 25 le processus de traitement de la commande du client, et avise celui-ci en 27.

La figure 4 illustre la troisième étape du procédé: le traitement d'un BEP postérieurement au paiement.

Il s'agit de la compensation des paiements. Le traitement effectué en 31 est identique au traitement de compensation des transactions par cartes, et n'est décrit ici que pour aider à la compréhension du processus complet.

A partir du détail des paiements enregistrés au cours de la journée, la plate-forme BEP (serveur ST) adresse en 32 à la banque commerçant (serveur SBF) le détail des paiements reçus par commerçant, afin que celle-ci puisse créditer leur compte en 33.

De même, la plarte-forme BEP adresse en 34 à la banque client (serveur SBC) le détail des transactions . La banque client connaît déjà les

transactions, mais cet envoi est destiné à lui permettre de vérifier en 35 le montant total débité (en cas de différence).

Enfin, la plate-forme BEP adresse en 36 à une banque de compensation BEP les écritures de débit et de crédit interbancaires afin de lui permettre de passer en 37 les écritures de compensation entre banques participantes.

Le procédé et le système décrits permettent de simplifier les techniques de sécurisation des paiements électroniques en s'affranchissant de la nécessité d'authentifier en ligne l'auteur du paiement. Les problèmes de sécurisation des échanges dans lesquels l'auteur du paiement est impliqué sont, pour l'essentiel, réduits à ce qui touche à la relation entre la banque et son client. La sécurité des échanges entre le serveur de traitement ST et le serveur SBC de la banque du client est en effet d'une autre nature car il s'agit là de professionnels. Les mécanismes mis en oeuvre sont suffisamment simples pour être facilement compris par les utilisateurs. Les clients ont la possibilité de gérer leur risque, par exemple en ne demandant l'attribution d'un BEP de valeur élevée qu'au moment du paiement, et les banques sont placées au coeur du processus de confiance.

Il va de soi que le mode de réalisation décrit n'est qu'un exemple et l'on pourrait le modifier, notamment par substitution d'équivalents techniques, sans sortir pour cela du cadre de l'invention.

C'est ainsi qu'une version simplifiée du système pourrait être dépourvue de serveur autonome de traitement des bons électroniques de paiement : en réponse à la proposition de paiement en 13, le client saisirait directement son code de BEP et retournerait ce code et la facture au serveur commerçant SF qui, à son tour, présenterait directement à la banque client (serveur SBC) la requête de validation du paiement. Dans ce cas, le serveur commerçant SF remplit partiellement les fonctions du serveur de traitement ST. Bien entendu, une telle version simplifiée n'offre pas les mêmes garanties de sécurité que celle décrite ci-dessus.

Selon une autre variante, le client pourrait introduire directement le code de son BEP dans la facture électronique émise par le serveur fournisseur SF, et celle-ci serait retournée ainsi complétée au serveur de

traitement ST qui contrôlerait alors l'identité du fournisseur. Faute d'identification du fournisseur, le serveur de traitement avertirait le client du refus de la transaction. Dans ce cas, suivant la configuration du système, le serveur de traitement ST ne présenterait pas de demande de validation au serveur SBC et le BEP pourrait être utilisé ultérieurement par le client pour un autre paiement ou, au contraire, par mesure de sécurité, ce BEP serait rendu inutilisable par sa présentation au serveur SBC.

REVENDICATIONS

1. Procédé de paiement électronique d'un fournisseur par un client via un réseau de communication, caractérisé en ce qu'il comprend les étapes de :

a) génération conditionnelle (6) par un établissement financier, en réponse à une requête dudit client, d'un code unique et non prédictible représentatif d'un bon de paiement de valeur maximale prédéterminée,

b) transmission (7) dudit code audit client,

c) stockage (8) par ledit établissement financier dans un serveur de paiement (SBC) de données représentatives dudit bon, lesdites données représentatives comprenant au moins ledit code, ladite valeur et des données d'identification dudit client,

d) transmission par ledit client, à un serveur (ST) de traitement de bon électronique, de données de paiement comprenant ledit code et une somme déterminée, en réponse à une demande de paiement de ladite somme émanant d'un fournisseur (SF), et,

e) validation conditionnelle, par ledit serveur de paiement (SBC), du paiement de ladite somme audit fournisseur en réponse à la transmission électronique (20) par ledit serveur de traitement (ST) d'une demande de validation dudit bon.

2. Procédé selon la revendication 1, caractérisé en ce que lesdites données de paiement comprennent des données d'identification dudit fournisseur (SF), ledit code et ladite somme, et ledit serveur de traitement (ST) :

* contrôle l'identité dudit fournisseur (SF) en réponse à la réception desdites données de paiement,

* transmet conditionnellement ladite demande de validation audit serveur de paiement (SBC), en fonction du résultat dudit contrôle, et

* transmet électroniquement audit fournisseur (SF) une information de validation de paiement de ladite somme en réponse à ladite validation dudit bon par ledit serveur de paiement (SBC).

3. Procédé selon la revendication 2, caractérisé en ce que ladite étape d) comprend :

d1) la transmission électronique, dudit fournisseur (SF) audit client (TC), d'une facture électronique comprenant ladite somme et des premières données d'identification dudit fournisseur et de ladite facture,

d2) la transmission électronique de ladite facture dudit client (TC) audit serveur de traitement (ST) en réponse au choix par ledit client de son règlement par un bon de paiement électronique,

d3) le contrôle de l'identité dudit fournisseur (SF) par ledit serveur de traitement (ST) au moyen desdites premières données d'identification en réponse à la réception de ladite facture,

d4) la construction et la transmission électronique audit client (TC), par ledit serveur de traitement (ST), d'un formulaire de paiement en réponse à la validation dudit contrôle de l'identité dudit fournisseur, ledit formulaire de paiement comprenant ladite somme et des secondes données d'identification dudit fournisseur et de ladite facture, et

d5) l'introduction dudit code dans ledit formulaire par ledit client (TC) pour constituer un message de paiement,

ledit serveur de traitement (ST) transmettant ladite demande de validation audit serveur de paiement (SBC) en réponse à la réception dudit message de paiement.

4. Procédé selon l'une quelconque des revendications 2 et 3, caractérisé en ce que ladite étape e) comprend la mise en oeuvre par ledit serveur de paiement (SBC) des opérations de :

e1) comparaison du code reçu dudit client (TC) via ledit serveur de traitement (ST) avec ledit code stocké à l'étape c),

e2) vérification que le bon représenté par ledit code stocké n'a pas été utilisé antérieurement, et

e3) comparaison de ladite somme à ladite valeur stockée à l'étape c).

5. Procédé selon la revendication 4, caractérisé en ce que :

- lesdites étape a) et c) comprennent l'attribution et le stockage par et dans ledit serveur de paiement (SBC) d'au moins une condition limitative relative au contexte d'utilisation dudit bon, et

- ladite étape e) comprend la vérification par ledit serveur de paiement (SBC) du respect par ladite demande de validation de ladite condition limitative attribuée audit bon.

6. Procédé selon la revendication 5, caractérisé en ce que ladite condition limitative appartient au groupe comprenant :

- une date de péremption dudit bon,
- une limitation de l'utilisation dudit bon dans le cadre d'une catégorie d'activité déterminée,
- une limitation de l'utilisation dudit bon pour le paiement d'au moins un fournisseur déterminé,
- l'association audit message transmis audit serveur de traitement (ST) d'une signature électronique dudit client.

7. Procédé selon la revendication 6, caractérisé en ce que ladite demande de validation comprend des données de datation générées par ledit serveur de traitement (ST) pour le contrôle par ledit serveur de paiement (SBC) de la date de péremption dudit bon.

8. Procédé selon l'une quelconque des revendications 1 à 7, caractérisé en ce que lesdites étapes a), b) et d) comprennent :

- la transmission électronique par ledit client, à partir d'un terminal (TC), de ladite requête audit serveur de paiement (SBC),
- la transmission électronique par ledit serveur de paiement (SBC) dudit code audit terminal (TC),
- la transmission électronique desdites données de paiement audit serveur de traitement (ST) à partir dudit terminal (TC).

9. Procédé selon l'une quelconque des revendications 1 à 8, caractérisé en ce que ladite transmission électronique est effectuée via un canal de communication sécurisé (R).

10. Système de paiement électronique pour la mise en oeuvre du procédé selon l'une quelconque des revendications 1 à 9, caractérisé en ce qu'il comprend :

- au moins un terminal (TC) d'accès d'au moins un client à une application de paiement électronique et à un réseau de communication (R),

- au moins un serveur de paiement (SBC) connecté audit réseau de communication et comprenant :
  * des moyens de génération conditionnelle dudit code pour la mise en oeuvre de ladite application,
  * des moyens de stockage desdites données représentatives dudit bon, et
  * des moyens de transmission dudit code audit terminal (TC),
- au moins un serveur fournisseur (SF) connecté audit réseau de communication (R) et comprenant des moyens d'élaboration et de transmission audit terminal, dans le cadre de ladite application, d'une facture susceptible d'être payée au moyen dudit bon, et
- au moins un serveur intermédiaire (ST) de traitement de bons électroniques comprenant :
  * des moyens (19) de construction d'un message de demande de validation dudit bon en réponse à la réception d'un message de paiement émanant dudit client,
  * des moyens (20) de transmission dudit message de demande de validation audit serveur de paiement (SBC), et
  * des moyens (24) de transmission audit serveur fournisseur (SF) d'une information de validation de paiement en réponse à la validation dudit bon par ledit serveur de paiement (SBC).

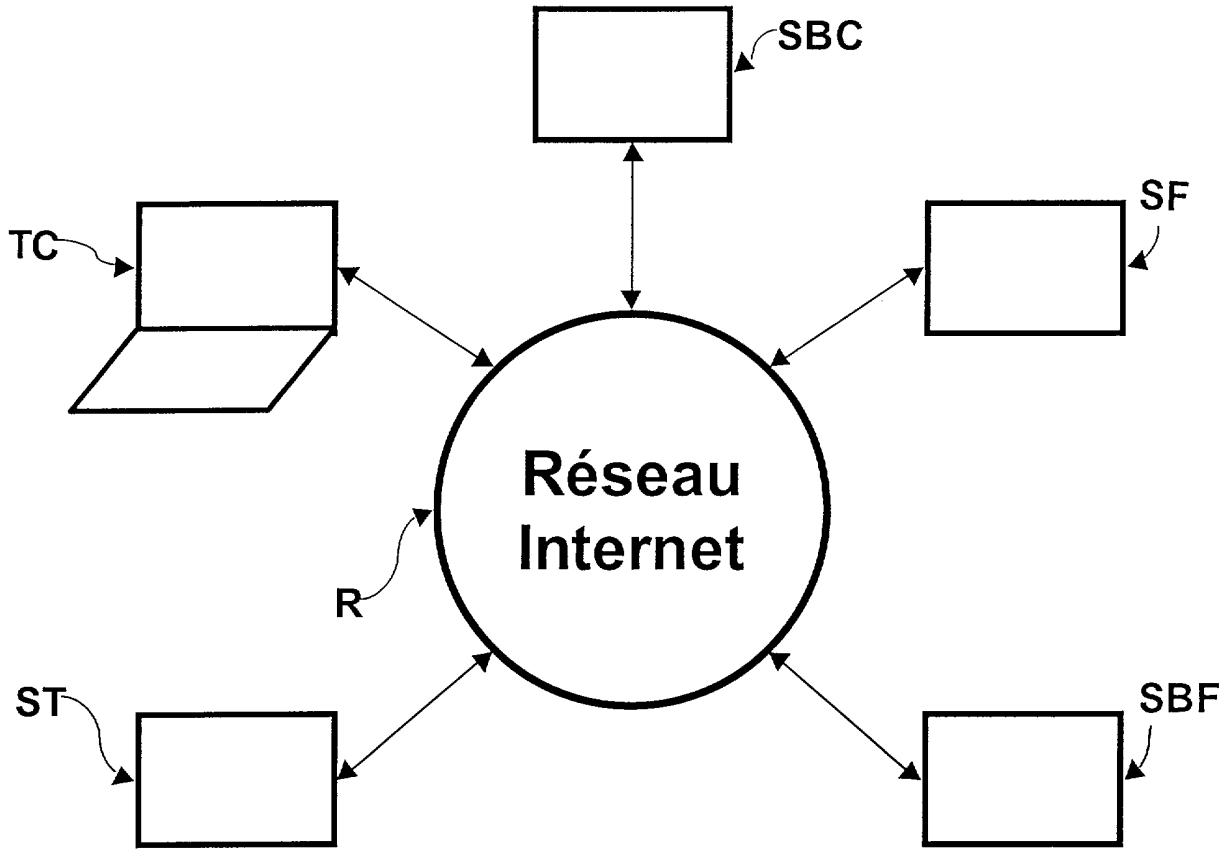


Figure 1

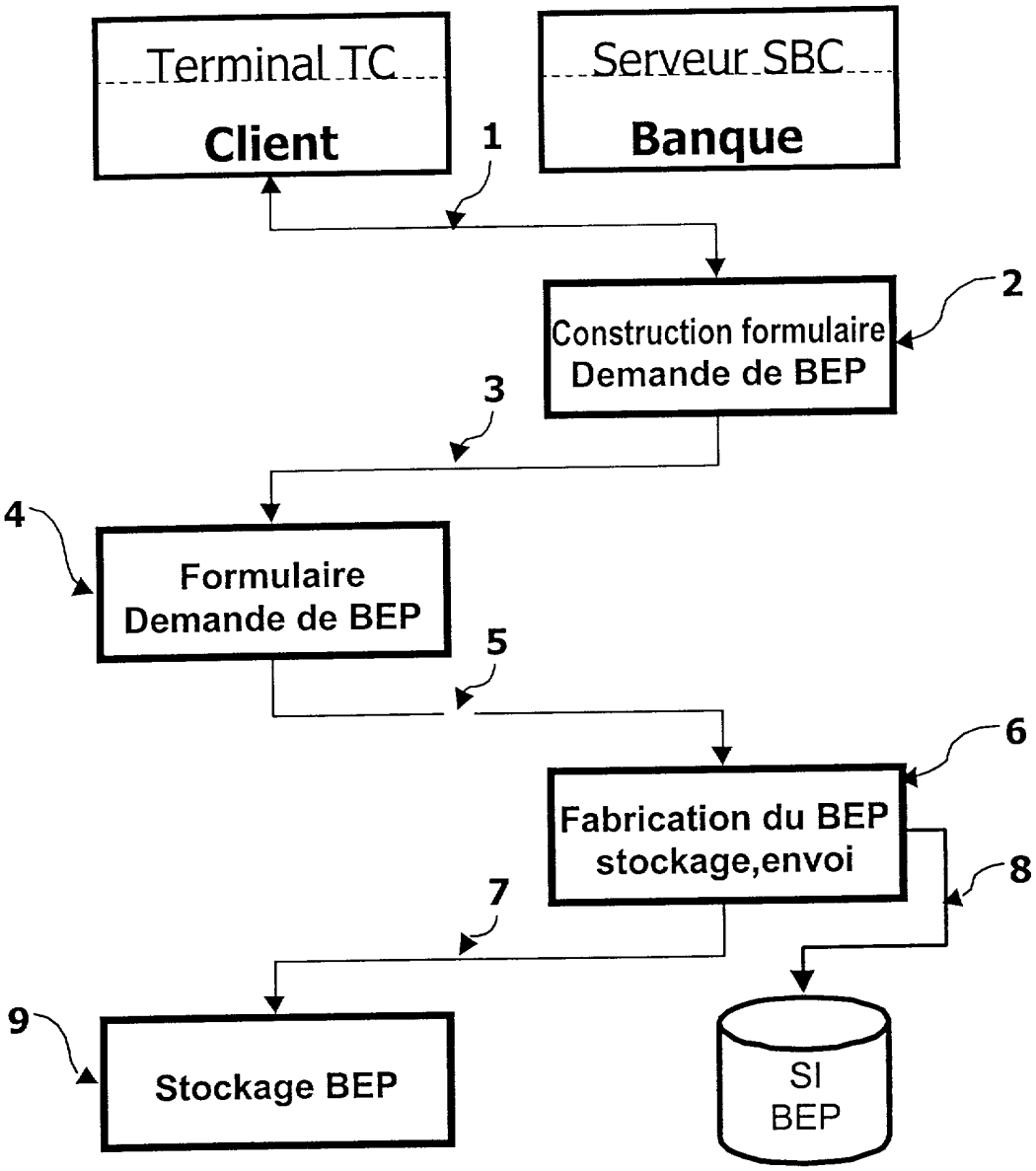

Terminal TC
Client
Serveur SBC
Banque
1
Construction formulaire
Demande de BEP
2
3
4
Formulaire
Demande de BEP
5
Fabrication du BEP
stockage,envoi
6
7
8
9
Stockage BEP
SI
BEP

Figure 2

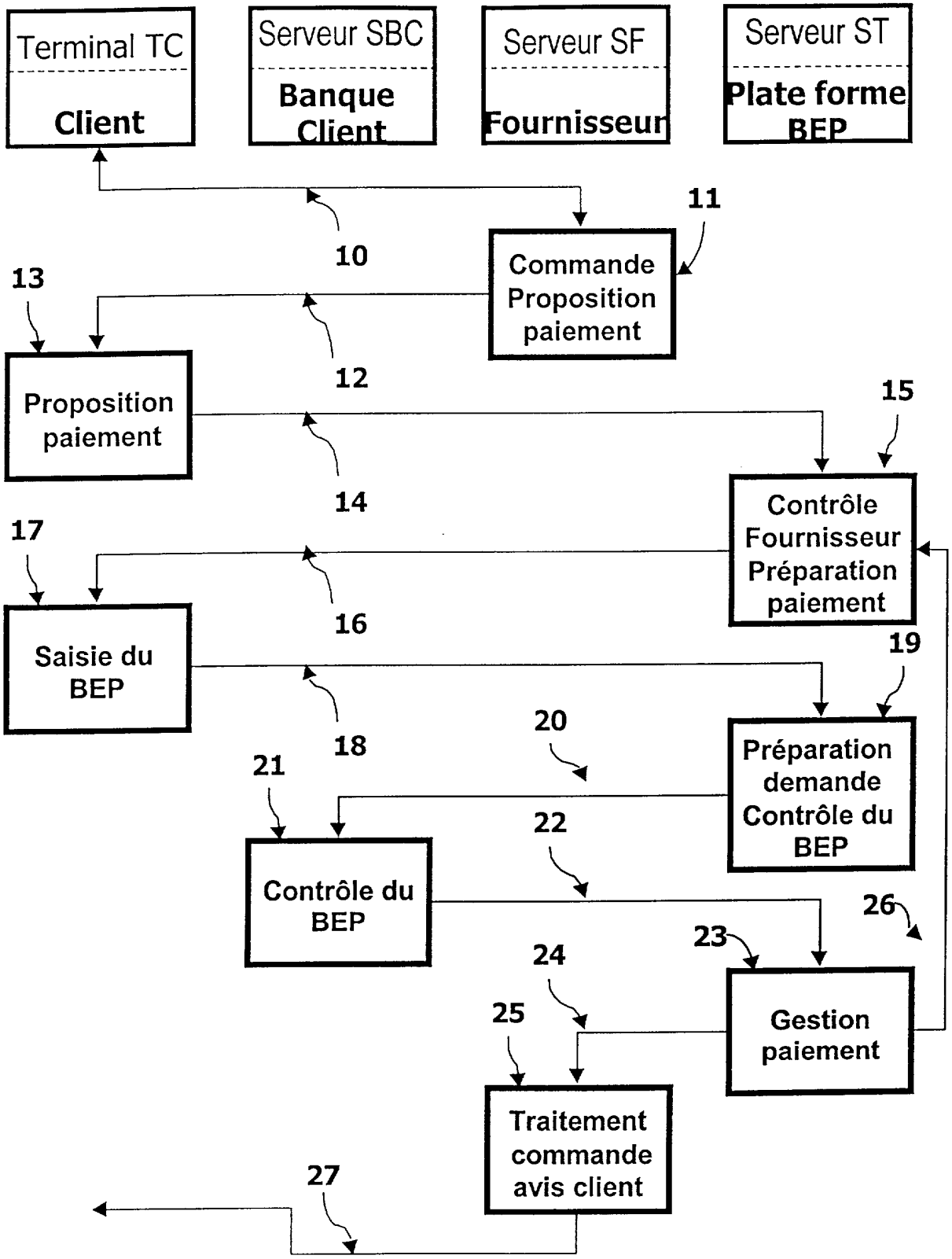

Terminal TC
Client
Serveur SBC
Banque Client
Serveur SF
Fournisseur
Serveur ST
Plate forme BEP
10
11
Commande Proposition paiement
13
12
Proposition paiement
15
14
Contrôle Fournisseur Préparation paiement
17
16
Saisie du BEP
19
18
20
Préparation demande Contrôle du BEP
21
22
Contrôle du BEP
26
23
24
25
Gestion paiement
Traitement commande avis client
27

Figure 3

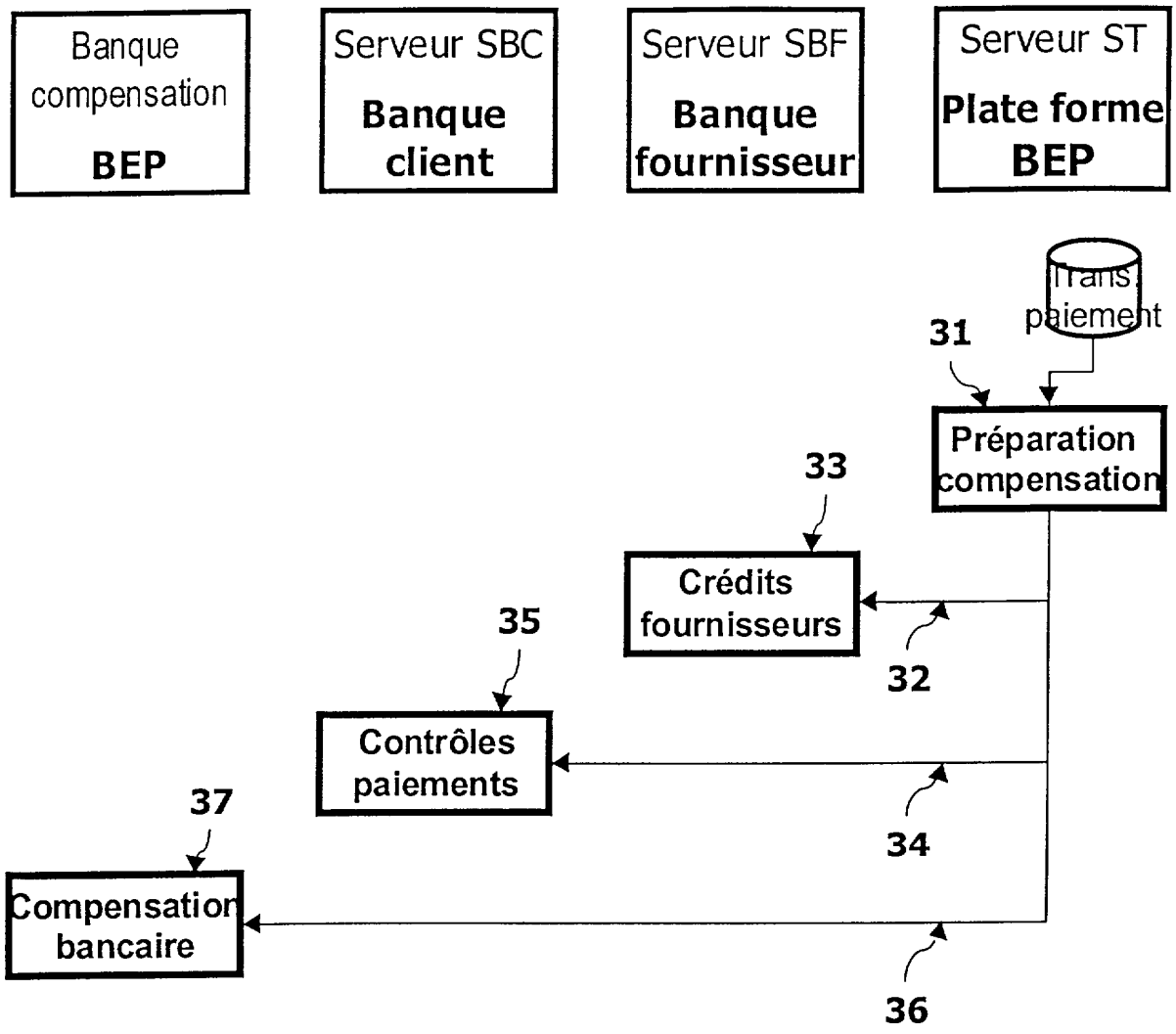

Banque compensation
BEP
Serveur SBC
Banque client
Serveur SBF
Banque fournisseur
Serveur ST
Plate forme BEP
Trans paiement
31
Préparation compensation
33
Crédits fournisseurs
32
35
Contrôles paiements
34
37
Compensation bancaire
36

Figure 4

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

2808144

N° d'enregistrement national

FA 587456
FR 0005109

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		
Y	US 5 883 810 A (ROSEN DANIEL ET AL) 16 mars 1999 (1999-03-16)	1,10	H04L9/00 G06F17/60
A	* colonne 4, ligne 24 - colonne 5, ligne 23; figures * * colonne 8, ligne 14 - colonne 11, ligne 40 *	5,6,8	
Y	US 5 920 847 A (KOLLING RAY ET AL) 6 juillet 1999 (1999-07-06)	1,10	
A	* colonne 27, ligne 28 - colonne 29, ligne 37; figures 12,13,19A-19C *	2,8	
A	US 5 677 955 A (ANDERSON MILTON M ET AL) 14 octobre 1997 (1997-10-14) * abrégé; revendications 2,13; figure 3 *	1,8-10	
A	US 5 715 314 A (MACKIE DAVID J ET AL) 3 février 1998 (1998-02-03) * colonne 5, ligne 16 - colonne 8, ligne 32; figures 2A-2I,3A-3B *	1,10	
A	WO 98 49658 A (CONKLIN FREDRICK SIDNEY ;PRINGLE STEVEN JOHN (US); BERG MICHAEL J) 5 novembre 1998 (1998-11-05) * page 19, ligne 23 - page 23, ligne 11; figures 11A-11D *	1-3,10	

DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)

G06F
G07F

Date d'achèvement de la recherche	Examinateur
8 février 2001	Paraf, E

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)