ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19)

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

(12) FASCICULE DE BREVET

(11) N° de publication :
MA 31343 B1

(51) Cl. internationale :
G06Q 20/00

(43) Date de publication :
03.05.2010

(21) N° Dépôt :
31299

(22) Date de Dépôt :
16.10.2008

(71) Demandeur(s) :
INSOFT, ESPACE PALMIER, 34 RUE CHARAM ACHAYKH, APPT. 7 20100 CASABLANCA (MA)

(72) Inventeur(s) :
BENIDER Abdellatif

(74) Mandataire :
ABDELLATIF BENIDER

(54) Titre : **PROCEDE SECURISE POUR LE PAIEMENT PAR VOIE ELECTRONIQUE**

(57) Abrégé : L'INVENTION PERMET D'EFFECTUER DES PAIEMENTS ÉLECTRONIQUES DE MANIÈRE COMBINANT À LA FOIS UN NIVEAU DE SÉCURITÉ ÉLEVÉ, UNE GRANDE PRATICITÉ ET UN FAIBLE COÛT DE TRANSACTION. A CETTE FIN , LE PROCÉDÉ UTILISE LE TÉLÉPHONE MOBILE COMME TERMINAL D'AUTORISATION DES PAIEMENTS ÉLECTRONIQUES EN Y AJOUTANT DES FONCTIONNALITÉS SPÉCIFIQUES. LE PROCÉDÉ EST AGNOSTIQUE ET PEUT ÊTRE DÉPLOYER DANS TOUS LES PAYS ET PAR TOUTE BANQUE SANS ÊTRE LIÉE À UN OPÉRATEUR DE TÉLÉCOMMUNICATIONS QUE CE SOIT AU NIVEAU TECHNIQUE OU COMMERCIAL. L'INVENTION PERMET DE RÉALISER LES PAIEMENTS RELATIFS À DES TRANSACTIONS ENTRE ACHETEUR ET VENDEUR, AUSSI BIEN DANS LE MONDE RÉEL : *DANS UN POINT DE VENTE *DANS LE CADRE DE LA DISTRIBUTION DE PRODUITS PHYSIQUES B2B2C, (EXEMPLE : TRANSACTIONS ENTRE PRODUCTEUR/DISTRIBUTEUR DE BNOISSONS GAZEUSES ET UNE ÉPICERIE) QUE DANS LE MONDE VIRTUEL : *SUR UN SITE WEB *SUR UN SITE WAP CES TRANSACTIONS PEUVENT CONCERNER DES PRODUITS PHYSIQUES OU DES PRODUITS NUMÉRIQUES. LE FAIBLE COÛT PAR TRANSACTION ENGENDRÉ PAR LE PROCÉDÉ LUI PERMET D'ÊTRE AUSSI BIEN VALIDE POUR LE MICRO-PAIEMENT QUE POUR LE MACRO-PAIEMENT. EN CAPITALISANT SUR LA LARGE DIFFUSION DU TÉLÉPHONE MOBILE ET SUR DES TECHNOLOGIES RÉPANDUES TELLES QUE LE SMS, LE PROCÉDÉ PERMET AINSI QUR DE RENDRE LES SERVICES DE PAIEMENT ÉLECTRONIQUE ACCESSIBLES À UNE LARGE POPULATION.

Résumé

L'invention permet d'effectuer des paiements électroniques de manière combinant à la fois un niveau de sécurité élevé, une grande praticité et un faible coût de transaction.

A cette fin, le procédé utilise le téléphone mobile comme terminal d'autorisation des paiements électroniques en y ajoutant des fonctionnalités spécifiques.

Le procédé est agnostique et peut être déployé dans tous les pays et par toute banque sans être liée à un opérateur de télécommunications que ce soit au niveau technique ou commercial.

L'invention permet de réaliser les paiements relatifs à des transactions entre acheteur et vendeur, aussi bien dans le monde réel :

- dans un point de vente,
- dans le cadre de la distribution de produits physiques B2B2C, (exemple : transactions entre producteur/distributeur de boissons gazeuses et une épicerie)

que dans le monde virtuel,

- sur un site web,
- sur un site WAP.

Ces transactions peuvent concerner des produits physiques ou des produits numériques.

Le faible coût par transaction engendré par le procédé lui permet d'être aussi bien valide pour le micro-paiement que pour le macro-paiement. En capitalisant sur la large diffusion du téléphone mobile et sur des technologies répandues telles que le SMS, le procédé permet ainsi de rendre les services de paiement électronique accessibles à une large population.

31343
03 MAI 2010

Procédé Sécurisé pour le Paiement par voie Électronique

Domaine de l'invention

Le procédé de l'invention permet aux clients d'une banque, d'un opérateur financier ou d'un opérateur de télécommunication de payer leurs achats et factures dans le monde physique ou virtuel en utilisant leur téléphone mobile. Il leur permet aussi d'effectuer des transferts d'argent entre eux. Le procédé améliore les procédés existant de paiement et de transfert d'argent électroniques en apportant une meilleure sécurité au processus d'autorisation de paiement tout en permettant un faible coût transactionnel et une plus grande accessibilité.

État de la Technique

Il existe aujourd'hui différents procédés de paiement électronique pour des transactions. Les plus répandus reposent sur la carte bancaire et l'infrastructure adéquate en termes de TPE (Terminal de Paiement Électronique), de serveurs monétiques et de réseau de transmission de données. L'utilisation de la carte à puce au lieu de la carte magnétique permet d'améliorer de manière substantielle la sécurité des transactions de paiement. Ces procédés sont bien adaptés au macro-paiement pour des transactions se déroulant dans le monde réel.

Depuis quelques années, des banques, groupement de banques, opérateurs de télécommunication, groupement d'opérateurs de télécommunication, groupement d'opérateurs de télécommunication et de banques, ont lancé de nouveaux moyens de paiement, basés sur des procédés de paiement électronique utilisant le téléphone mobile comme moyen d'initiation et/ou de validation du paiement.

Par exemple, des opérateurs offrent la possibilité au client d'autoriser des paiements électroniques par SMS. Pour effectuer le paiement, le client de ce service communique au vendeur son numéro de téléphone que ce dernier saisi sur son système de gestion des ventes ou son système de paiement électronique qui envoie à son tour une demande de paiement au système en charge du service. Ce dernier, envoie un SMS au client qui résume la transaction et lui demande de la confirmer en répondant par un SMS contenant son code PIN. Si le système de paiement électronique reçoit le bon code PIN, il autorise la transaction.

Ce procédé reste limité dans son application à des transactions de petite valeur ou présentant un faible risque de fraude à cause son faible niveau de sécurité. En effet, les éléments constituant de la transaction, et le PIN en particulier, sont transmis en clair dans certaines plates-formes des opérateurs de télécommunication. En plus, le code PIN reste enregistré dans le dossier des messages SMS et constitue donc une faille de sécurité non négligeable.

Dans d'autres procédés, on a remplacé le SMS par des échanges USSD mais le gain en sécurité reste insuffisant pour permettre tout type de transaction.

Il existe un autre procédé qui assure un niveau élevé de sécurité et qui est basé sur l'utilisation de la carte SIM du client pour héberger et exécuter une application PKI (public Key Infrastructure) permettant d'authentifier et signer les demandes de paiement provenant du système de paiement électronique.

Malheureusement, l'existence de contraintes logistiques pour la mise à niveau des cartes SIM des clients peut limiter la diffusion du service à une large population. En plus, le succès commercial de tout service utilisant ce procédé nécessite une forte collaboration entre l'organisme gestionnaire du service de paiement électronique et un ou plusieurs opérateurs de télécommunication.

En conclusion, même si les procédés actuels de paiement par téléphone mobile promettent d'apporter des avantages réels pour élargir le champs d'utilisation du paiement électronique au-delà des possibilités offertes par la carte bancaire et l'infrastructure associée, on constate que le paiement dit par mobile reste aujourd'hui peu disponible à l'échelle mondiale et encore limité aux achats de produits numériques et de certains produits physiques de faible valeur comme les tickets de parking.

Définition du problème à résoudre

Nous proposons d'élargir le champ d'utilisation du paiement électronique en mettant en place un *nouveau* procédé de paiement électronique qui a les caractéristiques suivantes :

1. Hautement sécurisé
2. Rapide
3. Pratique et toujours accessible
4. Pouvant être utilisé par une plus large population que les procédés actuels
5. Offrant un coût par transaction suffisamment faible pour une utilisation dans le micro-paiement (faible coût d'équipement, faible coût de télécommunication, faible coût de fonctionnement, faible nombre d'intervenants)
6. Permettant d'effectuer des paiements électroniques pour des transactions de vente B2C aussi bien dans le monde réel que dans le monde virtuel
7. Permettant d'effectuer des paiements électroniques pour des transactions de vente B2C de produits physiques ou numériques
8. Permettant d'effectuer des paiements électroniques pour des transactions de vente B2B dans le cadre de la distribution
9. Permettant d'effectuer des paiements électroniques pour le règlement des factures mensuels B2C
10. Permettant d'effectuer des paiements électroniques pour le l'achat de produits prépayé B2C

Description de l'invention

On présente dans ce qui suit une description détaillée de l'invention et de ses déclinaisons. La déclinaison considérée comme étant la plus importante par l'inventeur sera présentée avec un plus grand niveau de détail que les autres déclinaisons. Cependant, cette description s'entend comme un enseignement général sur les concepts de l'invention et ne doit pas être interprétée comme une limitation de l'invention à l'une ou à l'ensemble des déclinaisons présentées. L'inventeur considère qu'un spécialiste de l'état de la technique du domaine en question reconnaitra différentes variations et variantes possibles aux déclinaisons présentées.

L'inventeur considère que, d'un point de vue conceptuel, il existe trois déclinaisons principales du procédé :

1. Le paiement relatif à une transaction d'achat dans un environnement réel (relatifs par exemple aux transactions commerciales entre une personnes et un vendeur dans point de vente physique ou aux transactions commerciales entres une épicerie et les livreurs de ses fournisseurs),
2. Le paiement relatif à une transaction d'achat dans un point de vente virtuel (un site web par exemple) ou de paiement à distance (Paiement de factures récurrentes : eau/électricité, téléphone, internet, etc.),
   Transfert d'argent entre personnes.

Déclinaison 1 : transaction d'achat dans environnement physique
Pour décrire cette invention, nous nous plaçons dans le contexte d'un client faisant ses courses dans un point de vente physique et se présentant à la caisse pour régler ses achats. La personne à la caisse, qu'on appellera Vendeur dans la suite du document, a accès à un système de gestion des ventes incluant la gestion des encaissements par paiement électronique. Le vendeur saisi sur le système les différents articles présentés par le client, en général en utilisant un lecteur de code à barre, et crée une facture relative à cette transaction commerciale. A partir de cet instant, le procédé de notre invention peut être utilisé pour le paiement de cette transaction.

Nous pouvons aussi nous placer dans un contexte différent, néanmoins similaire d'un point de vue conceptuel, qui est le suivant : le livreur d'une entreprise de distribution de produits alimentaires se présente dans une épicerie dans le cadre de sa tournée périodique de vente et/ou livraison. Le livreur saisi la commande de l'épicerie (ou la valide si elle a été saisie préalablement), livre la marchandise et crée une facture relative a cette transaction. Le livreur dispose à cet effet, en général, d'un terminal portable relié à distance au système de gestion des ventes de son entreprise. A partir de cet instant, le procédé de notre invention peut être utilisé pour le paiement de cette transaction.

Pour décrire le procédé de paiement proposé par l'inventeur, nous utilisons le formalisme suivant :

Le client désigné par (C), ou Payeur (P), peut être une personne physique dans le cas de transactions B2C. Il peut aussi s'agir d'un employé d'une personne morale dans le cas de transactions B2B. Le client a souscrit à un service de paiement par mobile auprès d'un opérateur de paiement par mobile exploitant le procédé de la présente invention. Ce dernier peut être une banque, un organisme financier ou un opérateur de télécommunication.

Le Vendeur, ou (V), désigne tout représentant de l'entreprise (E), appelée aussi Bénéficiaire (BF), commercialisant des produits ou services et acceptant ce moyen de paiement, qu'il soit personne physique dans un point de vente ou une interface télématique (site web, serveur vocal interactif, etc.). (E) dispose d'un système de gestion des ventes (SGV) accessible par (V).

Le procédé repose sur trois composantes principales :

1. Une Application logicielle d'autorisation des paiements (A)

2. Un Serveur de d'Autorisation des Paiements par Mobile (S) connecté aux systèmes monétiques, systèmes d'autorisation bancaires ou au système de facturation de l'opérateur fournissant le service de paiement par mobile (B).
3. Un Serveur de gestion des utilisateurs du service (SGU)

(SGV) et connecté à (S) via un réseau de transmission de données sécurisé.

(A) présente les caractéristiques suivantes :

i. (A) est installée sur le téléphone mobile de (C).
ii. Le téléphone mobile de (C) est capable de recevoir des SMS
iii. (A) est capable de communiquer avec (S) d'une manière sécurisée grâce à un mécanisme de cryptage conforme à l'état de l'art en la matière utilisant une ou plusieurs clés symétriques et/ou asymétriques.
iv. Pour améliorer la sécurité du procédé, on peut envisager que (A) soit une application unique pour chaque client ou pour chaque groupe de clients. Dans ce cas, le système (SGU) activera l'application pour le client (C) lors de sa souscription au service. Cette activation pourra être faite par des mécanismes d'OTA (Over The Air) ou en utilisant un code d'activation qui associe au niveau des base de données de (SGU) chaque application (A) et ses clés de cryptage à un ou groupe de clients. En outre, la ou les clés utilisées par (A) peut ou peuvent être stockée(s) dans le code applicatif de (A) en variant sa/leurs position(s) dans le code applicatif de (A) d'un téléphone mobile à un autre, ou d'un groupe de téléphone mobile à un autre.

(C) dispose d'un code PIN confidentiel lui permettant d'autoriser ses paiements. Ce code est généré par (SGU) et communiqué à (C) lors de sa souscription au service de paiement par mobile.

Le procédé de paiement se présente comme suit (cf. Figure 1) :

1. (C) communique à (V) sa volonté d'utiliser son téléphone pour payer la facture en instance et lui communique son numéro de téléphone (ou un autre identifiant si nécessaire).
2. (V) saisie la demande de paiement sur le (SGV) en spécifiant le numéro du téléphone mobile communiqué par (C), le montant de la facture et le numéro de facture.
3. (SGV) envoie à (S) une demande de création de transaction de paiement en spécifiant le numéro du téléphone mobile communiqué par (C), le montant de la facture, le numéro de facture et l'identifiant du point de vente.
4. (S) effectue les opérations suivantes :
    a. (S) vérifie la recevabilité de la demande selon les règles de gestion établies par l'opérateur de paiement et les préférences du Client stockées sur le (SGU),
    b. (S) crée une nouvelle transaction de paiement de (E) par (C) relative au montant de la facture en spécifiant le numéro de facture et l'identifiant de point de vente. Le code de transaction est communiqué au (SGV) de (E),
    c. (S) extrait la clé de cryptage de (C) stockée sur le (SGU),
    d. (S) crée une clé temporaire de la transaction (β),
    e. (S) génère une demande d'autorisation de paiement incluant le (β) et des informations qualitatives sur la transaction telle que : le numéro de facture, le montant de la facture, le nom de l'entreprise (E), l'identifiant de point de vente,

f. (S) crypte la demande d'autorisation de paiement par clé de cryptage de (C),
5. (S) Envoi la demande d'autorisation de paiement crypté via SMS à (A),
6. (A) décrypte le message,
7. (A) informe (C) de la présence d'une demande paiement en :
    a. Affichant les détails qualitatifs de la transaction : le numéro de facture, le montant de la facture, le nom de l'entreprise (E) et l'identifiant de point de vente,
    b. Demandant d'introduire le code PIN pour accepter la transaction,
8. (C) saisie le code PIN,
9. (A) calcule le Code de confirmation de la transaction (α) en cryptant le code saisi par (C) par la clé de la transaction (β),
10. (A) confirme à (C) le paiement et affiche le Code de confirmation de la transaction (α),
11. (C) communique à (V) verbalement le Code de confirmation de la transaction (α),
12. (V) saisie (α) sur le (SGV),
13. (SGV) envoie à (S) une demande de validation de paiement de la transaction en cours en spécifiant le numéro de transaction et le code de confirmation de la transaction (α),
14. (S) effectue les opérations suivantes :
    a. vérifie que le client (C) a saisi le bon code PIN en recalculant le Code de Confirmation de la transaction (α) et en comparant avec le code (α) reçu par (S), et dans le cas de concordance, considère la demande de paiement autorisée par le client,
    b. Extrait les données bancaires de (C) stockées sur le (SGU),
    c. Extrait les données bancaires de (E) stockées sur le (SGU),
    d. Génère une transaction bancaire de paiement par (C) du montant de la facture au bénéfice de (E),
15. (S) envoie à (B) une demande de paiement par (C) du montant de la facture au bénéfice de (E),
16. (B) envoie à (S) la confirmation de la demande de paiement,
17. (S) envoie à (SGV) la confirmation de la demande de paiement,
18. (S) envoie à (A) la confirmation de la demande de paiement (optionnel).

Variantes possibles :

Il est possible de modifier le procédé décrit ci-dessus selon le besoin en apportant une ou plusieurs des modifications suivantes :

- L'application (A) et/ou ses clés de cryptages est/sont installée(s) sur la carte SIM de (C).
- La communication entre (S) et (A) se fait par DATA GPRS, 3G ou USSD.
- Pour améliorer la sécurité et la rapidité du procédé, en acceptant cependant d'augmenter les coûts de télécommunication, on peut le modifier à partir de l'étape 10 de la manière ci-après.

10. (A) confirme à (C) le paiement,
11. (A) envoie à (S) le Numéro de la transaction et le Code de confirmation de la transaction (α) cryptés par la clé de (C),
12. (S) effectue les opérations suivantes :

   a. Vérifie que le client (C) a bien saisi le Code PIN en vérifiant le Code de Confirmation de la transaction (α),
   b. Extrait les données bancaires de (C),
   c. Extrait les données bancaires de (E),
   d. Génère une transaction bancaire de paiement par (C) du montant de la facture au bénéfice de (E),
13. (S) envoie à (B) une demande de paiement par (C) du montant de la facture au bénéfice de (E),
14. (B) envoie à (S) la confirmation de la demande de paiement,
15. (S) envoie à (SGV) la confirmation de la demande de paiement,
16. (S) envoie à (A) la confirmation de la demande de paiement (optionnel).

Déclinaison 2 : transaction d'achat dans environnement virtuel
A la différence de la déclinaison 1, on se positionne ici dans un contexte où le client effectue son achat dans un point de vente virtuel à travers une interface télématique comme un site web ou un site wap. Dans ce cas, le procédé décrit dans la déclinaison 1 sera modifié légèrement de manière à éliminer l'interaction entre le client (C) et le vendeur (V) et la remplacer par une interaction entre le client et l'interface télématique proposée à cet effet par l'entreprise (E).

Déclinaison 3 : Transfert d'argent
A la différence de la déclinaison 1, on se positionne ici dans un contexte où le client souhaite transférer de l'argent à une autre personne, bénéficiaire (BF). Dans ce cas, les deux personnes doivent souscrire au service. Le procédé tel que présenté dans la déclinaison 1 est modifié de comme suit :

- Au lieu d'une initiation du processus par le bénéficiaire (étape 1,2 et 3 décrites dans la déclinaison 1), la demande de transfert d'argent est initiée par le Payeur et transmise au (S) à travers l'application (A) de son téléphone mobile. Pour cela, le Payeur saisi sur l'interface utilisateur de (A) le montant à transférer et le numéro de téléphone du destinataire,
- Les échanges entre (S) et (SGV) sont remplacés par des échanges entre (S) et l'Application (A') installée sur le téléphone mobile du bénéficiaire.

Exemples d'application

1. Paiement dans les supermarchés
2. Paiement dans les magasins modernes (franchises internationales, etc.)
3. Paiement des produits prépayés : eau et électricité dans les pays en développement, ticket de parking, téléphonie, accès internet, accès wifi
4. Paiement des produits numériques : passe d'accès à un journal en ligne, musique,
5. Paiement dans le monde virtuel : paiement de frais administratifs (egov),
6. Paiement de facture : eau/électricité, téléphone, internet, etc.
7. Paiement B2B : entre épicerie et ses fournisseurs.
8. Transfert d'argent entre personnes.
9. Retrait et mise à disposition d'argent sur un guichet automatique bancaire

Revendications

1. Un procédé, offrant à un Client (C) d'un opérateur de télécommunication, ou d'un organisme financier et d'un opérateur de télécommunication, des services de paiement électronique et de transfert d'argent, entre lui-même en tant que payeur (P) et un bénéficiaire (BF), et utilisant un téléphone mobile et un réseau de télécommunications mobile, et caractérisé par :
    a. un serveur d'autorisation des paiements par mobile (S) capable, premièrement de recevoir des demandes de paiement de la part de (BF), deuxièmement de vérifier leur recevabilité aussi bien par des procédés propres qu'en collaboration avec des systèmes appartenant à des organismes financiers ou des opérateurs de traitement des paiements électroniques, troisièmement de demander au payeur (P) d'autoriser la dite demande de paiement en utilisant un Protocole sécurisé d'autorisation impliquant des échanges avec le payeur et le bénéficiaire ;
    b. un téléphone mobile doté d'une application, spécifique ou standard, installée et exécutée sur le téléphone mobile du client (C) ou sur la carte SIM du client (C) ou composée de deux composantes dont l'une est installée sur le dit téléphone mobile et l'autre est installée sur la dite carte SIM, capable, premièrement de crypter et décrypter des messages, deuxièmement d'interagir avec (P), troisièmement de communiquer avec le serveur (S) en utilisant le dit Protocole.
2. Un procédé, offrant des services de paiement électronique et de transfert d'argent, utilisant un téléphone mobile et un réseau de télécommunications mobile, incluant les éléments caractérisant de la revendication 1 et utilisant un protocole d'autorisation permettant au serveur (S) d'obtenir l'autorisation du payeur (P) relative à une demande de paiement à, ou de transfert d'argent vers, le bénéficiaire (BF), et caractérisé par les étapes suivantes :
    a. A la réception de chaque demande de paiement, (S) crée une clé temporaire (β) de la transaction,
    b. (S) génère une demande d'autorisation de paiement incluant (β) et des informations qualitatives sur la transaction (telles que le numéro de facture, le montant de la facture, le nom de l'entreprise (E), l'identifiant de point de vente),
    c. (S) crypte la demande d'autorisation de paiement par la clé de cryptage de (C),
    d. (S) envoie la demande d'autorisation de paiement par SMS au téléphone mobile du client (C).
    e. le téléphone mobile du client (C) reçoit la demande d'autorisation de paiement qui est interceptée par l'application mobile (A)
    f. (A) informe (C) de la présence d'une demande paiement en affichant les détails qualitatifs de la transaction (tels que le numéro de facture, le montant de la facture, le nom de l'entreprise (E), l'identifiant de point de vente, dans d'un paiement en faveur d'une entreprise (E) ou le numéro de transfert, le montant, le nom et le numéro de téléphone du bénéficiaire dans le cas d'un transfert d'argent), et demande au client (C) d'introduire le code PIN pour accepter la transaction,
    g. (A) extrait la clé temporaire de la transaction (β), calcule le Code de confirmation de la transaction (α) en cryptant le code saisi par (C) par la clé de la transaction (β), et le communique au payeur (P).

h. Dans le cas de transfert d'argent, (C) communique à (BF) le Code de confirmation de la transaction (α), et dans le cas d'un paiement, (C) communique le Code de confirmation de la transaction (α) au (SGV) de (BF), directement ou via le vendeur représentant de (BF),
i. A la réception de (α), (B) dans le cas de transfert d'argent, ou le (SGV) de (BF) dans le cas d'un paiement, envoie à (S) une demande de validation de paiement de la transaction en cours en spécifiant le code de confirmation de la transaction (α),
j. A la réception par (S) d'une demande de validation de paiement, (S) vérifie que le client (C) a saisi le bon code PIN en recalculant le Code de Confirmation de la transaction (α) et en comparant avec le code (α) reçu par (S), et dans le cas de concordance, considère la demande de paiement autorisée par le client.

3. Un procédé, offrant des services de paiement électronique et de transfert d'argent, utilisant un téléphone mobile et un réseau de télécommunications mobile, incluant les éléments caractérisant de la revendication 1 et 2, et caractérisé par :
   a. la possibilité que l'application mobile (A) du téléphone mobile du client (C) envoie directement à (S) par SMS la demande de validation de paiement en spécifiant le Numéro de la transaction et le Code de confirmation de la transaction (α) cryptés au lieu de la transmettre via le bénéficiaire (BF) ou le (SGV) de (BF),
   b. la possibilité d'utiliser un autre moyen de communication que le SMS pour la communication entre (A) et (S) tels que et non limité à USSD ou le protocole IP sur GPRS ou 3G.

Schémas

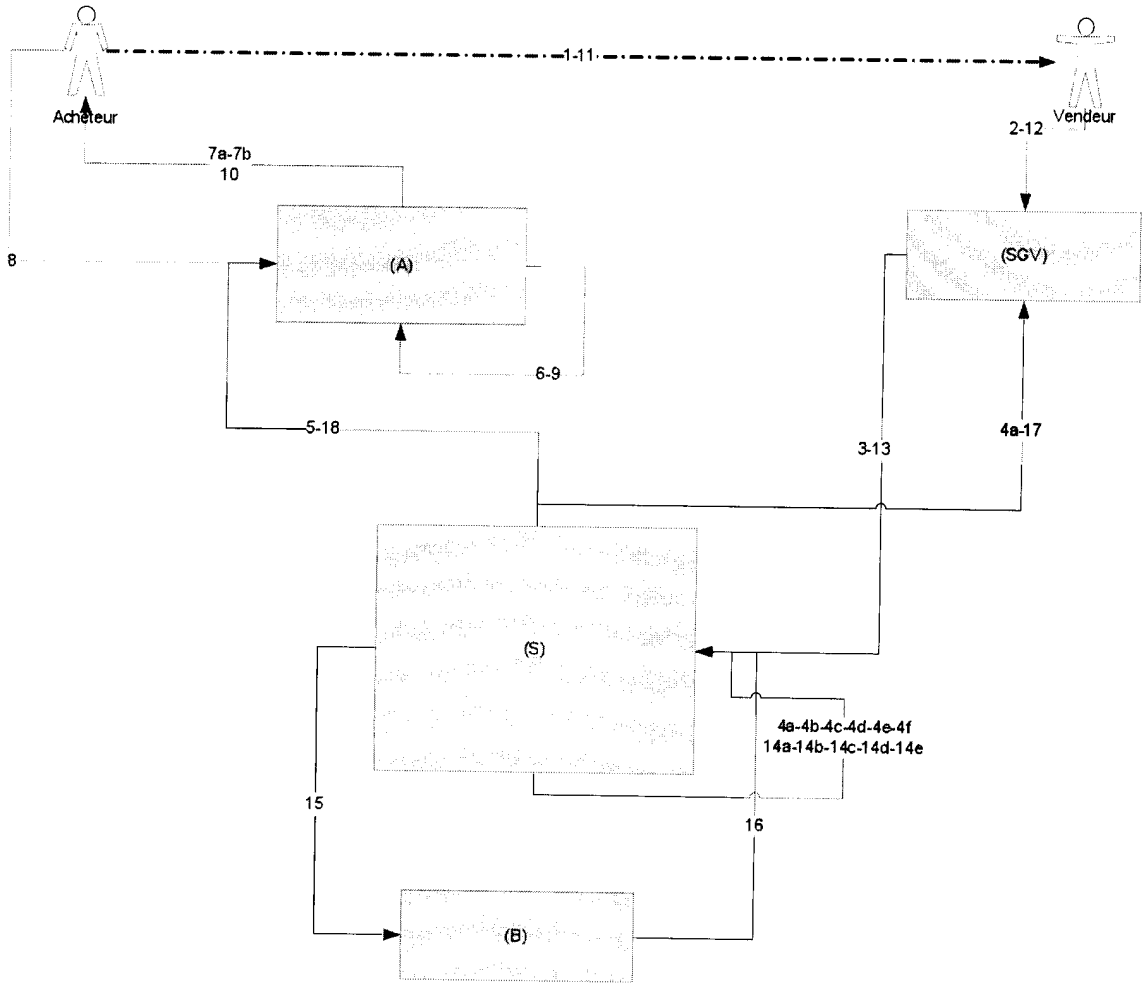

Figure 1: Schéma Transactionnel du Procédé (Déclinaison 1)