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 37139 A1

(51) Cl. internationale :
G06Q 20/00

(43) Date de publication :
29.01.2016

(21) N° Dépôt :
37139

(22) Date de Dépôt :
17.06.2014

(71) Demandeur(s) :
Université Hassan II Casablanca, (MA)

(72) Inventeur(s) :
MEDROMI HICHAM ; elismaili houssam ; TALLAL saadia

(74) Mandataire :
MAJID Sanaa

(54) Titre : **Conception et implémentation d'un protocole de paiement électronique sécurisé SEP**

(57) Abrégé : Le nouveau protocole repose sur Fenregistrement des parties prenantes dans la chaine E- commerce. La transaction est initiee par le detenteur d'une carte bancaire, elle contient des données sur l'ordre d'achat et les informations de paiement. L'ordre d'achat est traite par le comrnercant et les informations de paiement sont routees vers la banque du client de facon transparente pour le commercant et la passerelle de paiement. Les informations transmis sont cryptees afin de rendre la comprehension du message transmis impossible a toute personne qui n'a pas la cle du chiffrement. Un Hash est ajoute a toute message transmis entre les entites de la chaine E-commerce afin d'eviter aucune alteration ou destruction volontaire ou accidentelle, et conservent un format permettant leurs utilisation. Pour éviter la non-repudiation, le porteur utilise un jeton ou mot de passe, il pennet d'authentifier le porteur au pres de sa banque, cette etape est execurée directement entre le porteur et sa banque sans faire appel ai une partie tierce comme VISA ou MasterCard (contraireinent et 3D- Secure). Dans ce protocole, la transaction de paiement passe par deux etapes principales : la demande d'autorisation et Vauthentification du porteur. La premiere etape consiste a authentifier les parties prenantes, Verifier l'ordre d'achat par le commercant et Verifier les informations de paiement. La deuxieme etape consiste a authentiiier le porteur de carte aupres de sa banque et faire le paieinent en faveur du commercant.

Conception et implémentation d'un protocole de paiement électronique sécurisé

Le nouveau protocole repose sur l'enregistrement des parties prenantes dans la chaine E-commerce. La transaction est initiée par le détenteur d'une carte bancaire, elle contient des données sur l'ordre d'achat et les informations de paiement. L'ordre d'achat est traité par le commerçant et les informations de paiement sont routées vers la banque du client de façon transparente pour le commerçant et la passerelle de paiement. Les informations transmis sont cryptées afin de rendre la compréhension du message transmis impossible à toute personne qui n'a pas la clé du chiffrement. Un Hash est ajouté à toute message transmis entre les entités de la chaine E-commerce afin d'éviter aucune altération ou destruction volontaire ou accidentelle, et conservent un format permettant leurs utilisation.

Pour éviter la non-répudiation, le porteur utilise un jeton ou mot de passe, il permet d'authentifier le porteur au prés de sa banque, cette étape est exécutée directement entre le porteur et sa banque sans faire appel à une partie tierce comme VISA ou MasterCard (contrairement à 3D-Secure).

Dans ce protocole, la transaction de paiement passe par deux étapes principales : la demande d'autorisation et l'authentification du porteur. La première étape consiste à authentifier les parties prenantes, vérifier l'ordre d'achat par le commerçant et vérifier les informations de paiement. La deuxième étape consiste à authentifier le porteur de carte auprès de sa banque et faire le paiement en faveur du commerçant.

Conception et implémentation d'un protocole de paiement électronique sécurisé

L'invention concerne la conception d'un protocole de paiement électronique qui répond aux exigences de la sécurité des transactions d'achat en ligne.

Le E-commerce ou vente à distance est une activité qui se concentre sur le processus d'achat, par le biais d'un moyen électronique tel qu'Internet. Cela permet à une entreprise de vendre ses produits ou ses services de manière permanente à des marchés jusque-là inaccessibles, leur offrant ainsi une plus grande reconnaissance de la marque avec des coûts bien inférieurs aux solutions traditionnelles comme le déploiement de campagnes publicitaires coûteuses et l'ouverture de nouvelles succursales.

Le paiement en ligne est l'étape la plus critique et cruciale dans la chaine E-commerce, c'est le moyen permettant d'effectuer des transactions financières sur Internet.

La sécurité revêt une dimension majeure lorsqu'il s'agit d'échanger de l'information et de fournir des services commerciaux sur Internet. La crainte d'une brèche de sécurité est sans doute le plus grand obstacle à la pleine participation du public et des entreprises au commerce électronique sur internet.

Les exigences de la sécurité des transactions de paiement électronique sont : la confidentialité, l'intégrité des données, l'authentification des participants et la non-répudiation.

Actuellement, les mesures de sécurité se résument en l'utilisation des protocoles cryptographiques. Ces protocoles permettent au moyen de la cryptographie de véhiculer sur le réseau Internet des informations confidentielles sans qu'elles soient lisibles par des individus malveillants qui prennent un plaisir pour voler et saccager les vitrines des autres.

Secure Socket Layer (SSL) est le protocole le plus utilisé pour crypter les messages entre les navigateurs Web et les serveurs Web. SSL est aussi largement utilisé par les commerçants pour protéger les informations confidentielles des porteurs de carte (numéro de la carte, date expiration, ...) durant la transmission. SSL permet d'assurer l'intégrité et la sécurité des données échangées sur internet. Le problème majeur de SSL c'est que le commerçant est en possession des informations confidentielles du porteur, aussi SSL ne prévient pas du problème de la non-répudiation.

Le protocole SET (Secure Electronic Transaction) est venu pour résoudre les faiblesses de SSL, SET assure l'intégrité, la confidentialité et l'authentification du porteur et du commerçant. Malheureusement, SET n'as pas connu un grand essor à cause de la complexité d'installation et le coût de distribution des certificats de sécurité. Pour traiter cela, Visa introduit le protocole 3D-Secure, il repose sur la mise en place d'un contrôle supplémentaire lors de l'achat en ligne en complément des données bancaires classiquement saisies, l'acheteur devra valider sur une nouvelle fenêtre son paiement en saisissant une donnée secrète convenue avec sa propre banque.

Le but de la présente invention est de proposer un protocole de paiement électronique qui permet de garantir une sécurité élevée des transactions d'achat en ligne sans impliquer une partie tierce Visa ou MasterCard. Notre protocole répond aux exigences de la sécurité. Ce protocole évite les complexités d'implémentation contrairement à SET et 3D-Secure, il repose sur l'utilisation d'une autorité de certification pour vérifier l'identité des participants. La description standard du protocole est illustrée dans la figure 1.

Pour simplifier l'explication du fonctionnement et l'implémentation du protocole, nous utiliserons les notations suivantes :

C : Porteur

M : Commerçant

PG : Passerelle de paiement

IB : Banque du porteur

CA: Autorité de certification

Vshop : Site d'achat en ligne

PAN: Numéro de la carte crédit

CVV2: Card Verification Value or Cryptogramme (trois digits)

ExD: Date expiration de la carte

OI: Ordre d'achat

PI: Instructions de paiement

OIMD: Condensé de OI

PIMD: Condensé de PI

POMD: Condensé de OI et PI

K: Clé symétrique généré aléatoirement

Kum: Clé publique du commerçant

Kupg: Clé publique de la passerelle de paiement

Kuis: Clé publique de la banque du client

Krm: Clé privé du commerçant

Krpg: Clé privé de la passerelle de paiement

Kris: Clé privé de la banque du client

S: Signer

E: Crypter

D: Décrypter

V: Vérifier la signature

H: Hash

||: Concaténation

#: Dé concaténation

Eq: Egale

 : Certificat de sécurité

Le protocole assurera le déroulement de la transaction d'achat en ligne selon le scénario suivant :

1) Processus d'enregistrement : Avant de commencer une transaction, le commerçant, la passerelle de paiement et la banque du client devraient s'enregistrer et obtenir des certificats de sécurités auprès de l'autorité de certification. Le porteur de la carte devrait s'enregistrer et obtenir un mot de passe ou jeton auprès de sa banque.

2) La demande d'achat : le porteur de la carte se connecte au site internet du commerçant, il sélectionne les articles à acheter, puis il obtient un ordre d'achat qui contient les articles choisis. Le porteur envoie au commerçant sont ID local et un numéro généré aléatoirement afin de vérifier les certificats de sécurité du commerçant et de la passerelle de paiement. Alors, le porteur génère un OI encrypté, PI encrypté et la signature duale. La signature duale est cryptée sous une clé symétrique générée aléatoirement (voir figure 2). Afin d'éviter les complexités de distributions des certificats pour les clients, ces derniers ne sont pas obligés de les avoir. Le porteur de la carte prépare et envoie la demande d'achat au commerçant (voir figure 3). Le commerçant extrait la clé symétrique, traite OI et transmit PI encrypté à la passerelle de paiement (voir figure 4).

3) La demande d'autorisation : le commerçant signe et envoie la demande d'autorisation à la passerelle de paiement, il envoie la clé symétrique de la signature dual et PI encrypté. La demande d'autorisation est cryptée sous une autre clé symétrique. La passerelle de paiement vérifie la signature duale et obtient PI (voir figure 4). La passerelle de paiement transmit la demande d'autorisation et PI à la banque du client à travers un réseau interbancaire sécurisé (voir figure 5).

4) La réponse de la demande d'autorisation : la banque du client vérifie PI et la demande d'autorisation, elle exécute des contrôles pour s'assurer que le porteur est autorisé à faire cette transaction. La banque du client envoie la réponse de la demande d'autorisation avec son certificat de sécurité à la passerelle de paiement (voir figure 6). La réponse contient deux informations le code réponde et le code action. Le code réponse indique si la demande d'autorisation est approuvée ou non, le code action indique si le porteur de la carte est sollicité d'être authentifié au prés de sa banque par son mot de passe. La passerelle de paiement signe et envoie la réponse de la demande d'autorisation et le certificat de la banque du client au commerçant (voir figure 7). Le commerçant vérifie le code action, si le code est égale à 'Y', qui signifie que le client doit être authentifié par sa banque, le commerçant envoie une demande d'authentification au porteur contenant le certificat de la banque et des données d'autorisation (voir figure 8).

5) La demande d'authentification du porteur : le porteur vérifie le certificat de sa banque et envoie son mot de passe crypté sous une clé symétrique (voir figure 9). Le commerçant vérifie les données de la demande et transmit le mot de passe crypté à la passerelle de paiement (voir figure 10). La passerelle de paiement vérifie les données de la demande, le condensé du mot de passe et le transmit le mot de passe crypté à la banque du client. Cette dernière décrypte et

vérifie le mot de passe (voir figure 11).

6) La réponse de la demande d'authentification du porteur : la banque du client débite le compte du porteur par le montant de la transaction et envoie la réponse à la passerelle de paiement (voir figure 12). La passerelle de paiement transmit la réponse au commerçant (voir figure 13). le commerçant vérifie la réponse et fournit les articles ou les biens demandés au porteur.

Revendications

1. Une transaction de paiement en ligne se fait en deux étapes. La première étape consiste à vérifier la carte par sa banque émettrice, la deuxième étape concerne la vérification de l'identité du porteur.

2. La vérification de la carte consiste à vérifier la validité de la carte. Le porteur de carte transmit ses informations confidentielles numéro de carte, date expiration et le cryptogramme au commerçant, ce dernier transmit ces informations à la passerelle de paiement, puis à la banque du porteur.

3. La vérification de l'identité du porteur se fait directement entre le porteur et sa banque sans passer par une partie tierce. Le mot de passe du porteur est envoyé crypté à sa banque, seule cette dernière est capable de le décrypter.

4. Les informations sur l'article à acheter sont envoyées du porteur au commerçant dans un format crypté. Seul le commerçant peut vérifier ces informations.

5. Pour assurer la confidentialité, les données transmises sont séparées en deux parties : l'ordre d'achat et les instructions de paiement. L'ordre d'achat contient des informations concernant le produit à acheter, alors que les instructions de paiement contiennent les données confidentielles du porteur. L'ordre d'achat est crypté sous la clé publique du commerçant. Les instructions de paiement sont cryptées sous la clé publique de la passerelle de paiement. Ces deux données sont concaténées puis envoyées au commerçant. Le commerçant décrypte l'ordre d'achat et transmis les instructions de paiement cryptées à la passerelle de paiement. Cette dernière est la seule entité capable de décrypter les instructions de paiement.

6. Pour assurer l'intégrité de l'ordre d'achat et les instructions de paiement, une signature duale est générée, puis crypté sous une clé symétrique échangée entre le porteur et le commerçant, donc sans avoir besoin d'un certificat de sécurité pour le client, cela facilite le déploiement et l'utilisation du protocole.

Figures

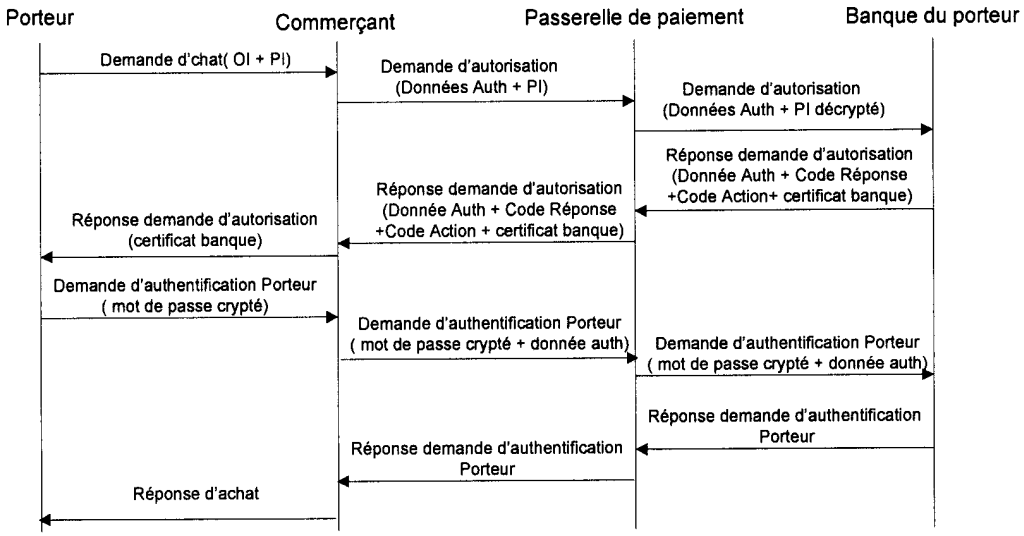

Figure 1

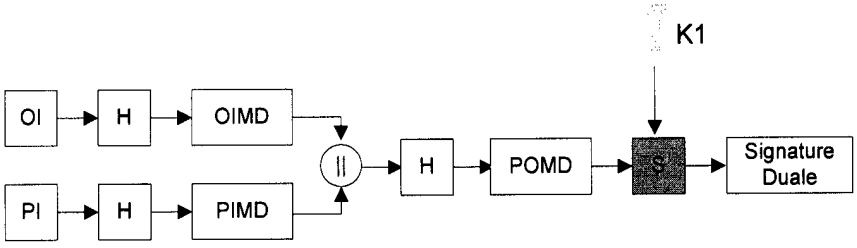

Figure 2

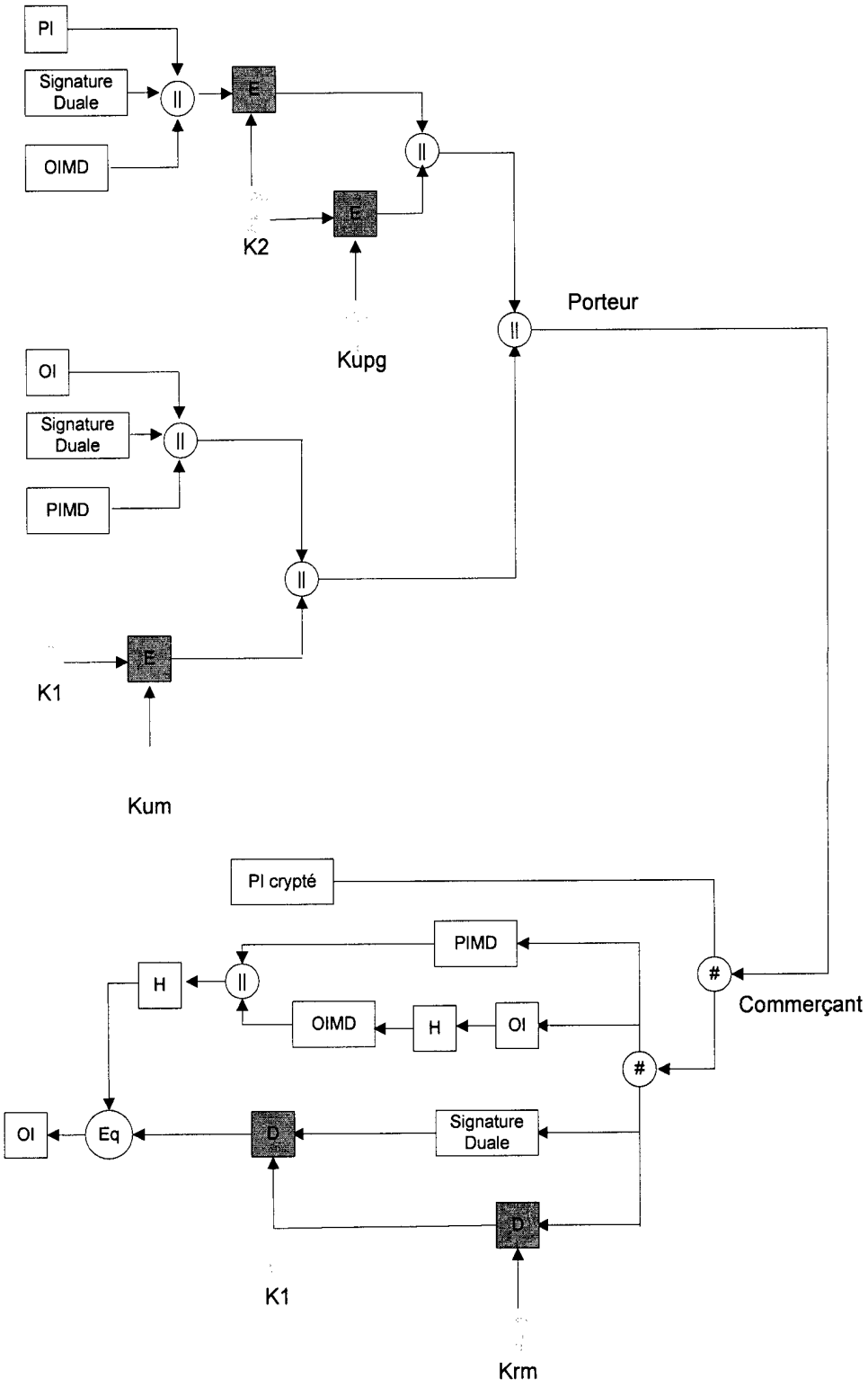
PI
Signature Duale
OIMD
E
K2
Kupg
Porteur
OI
Signature Duale
PIMD
K1
Kum
PI crypté
PIMD
H
OIMD
H
OI
Commerçant
OI
Eq
D
Signature Duale
K1
Krm

Figure 3

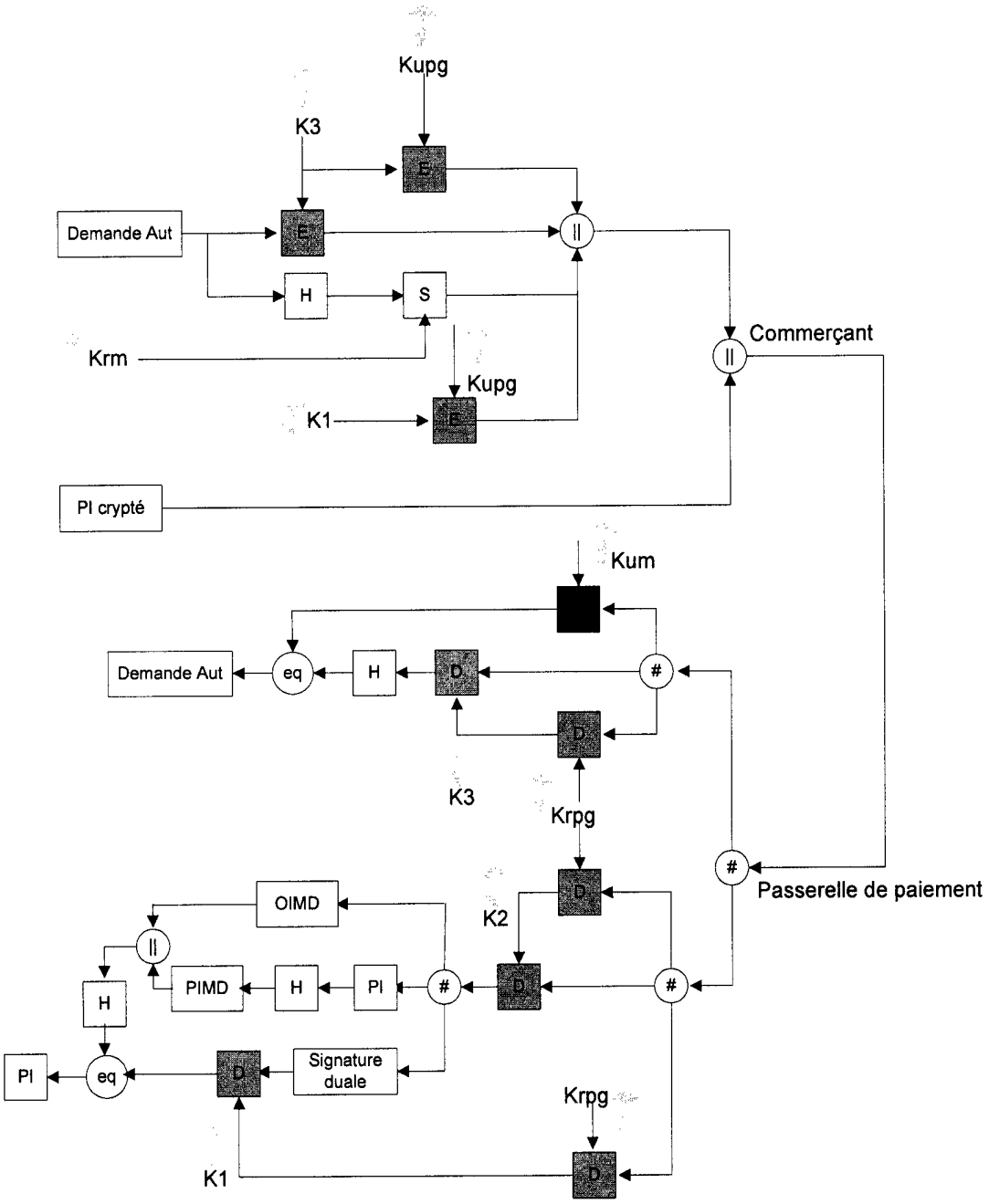

Figure 4

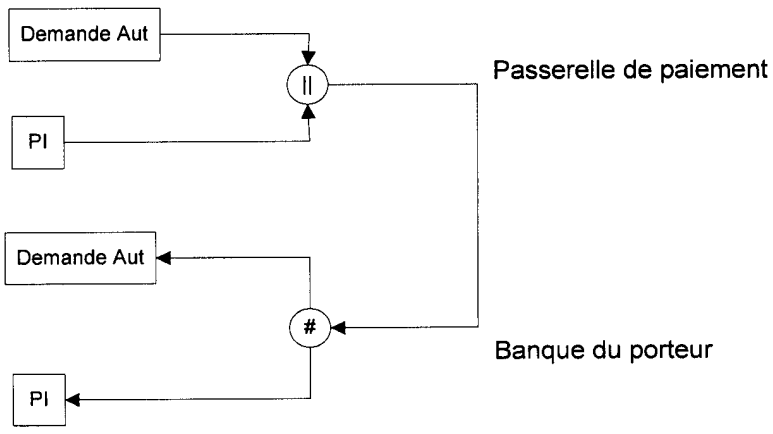

Figure 5

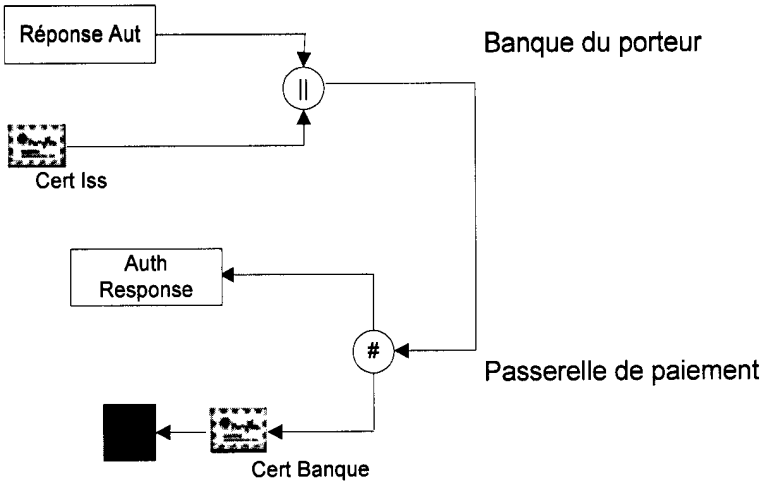

Figure 6

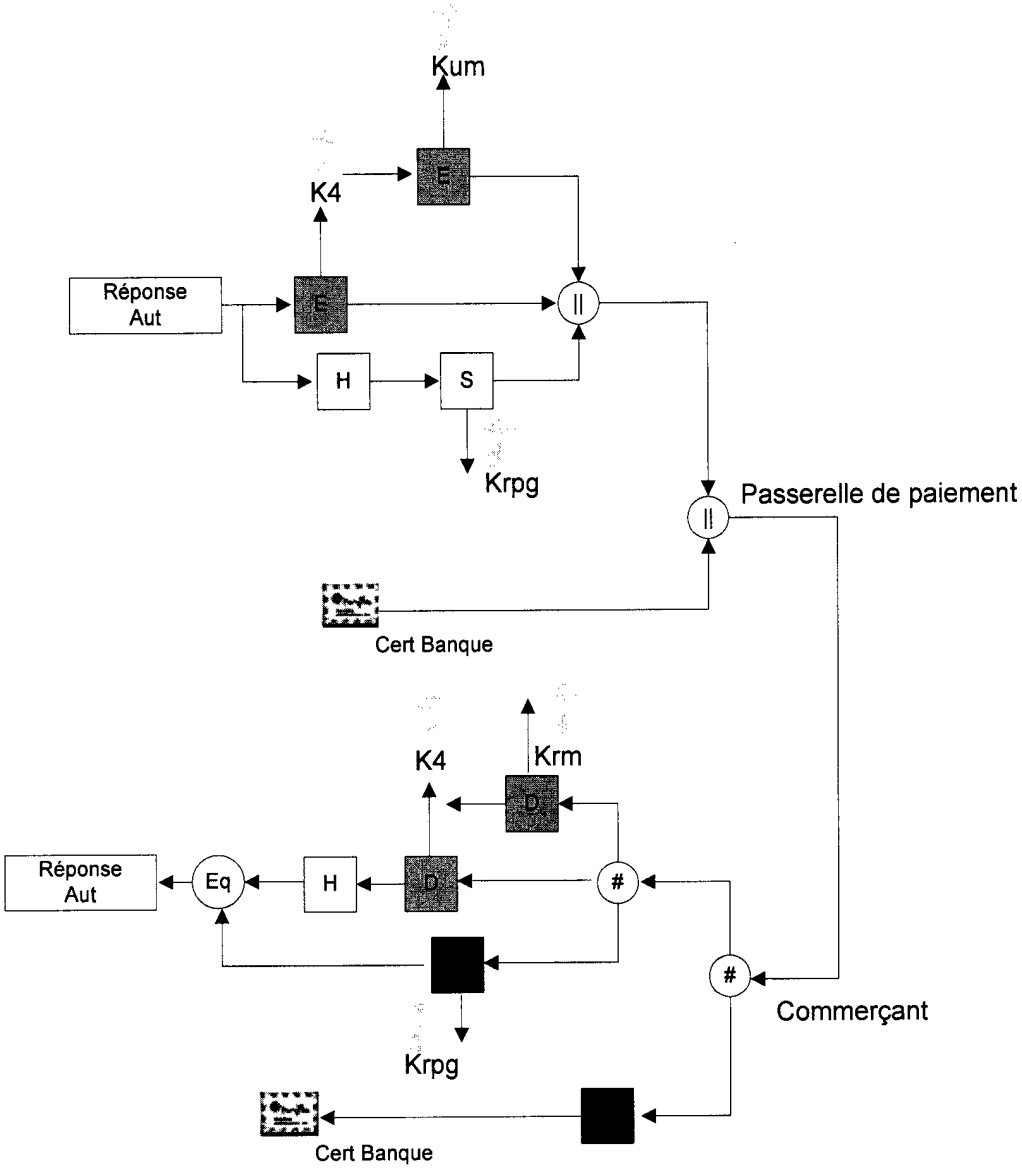

Figure 7

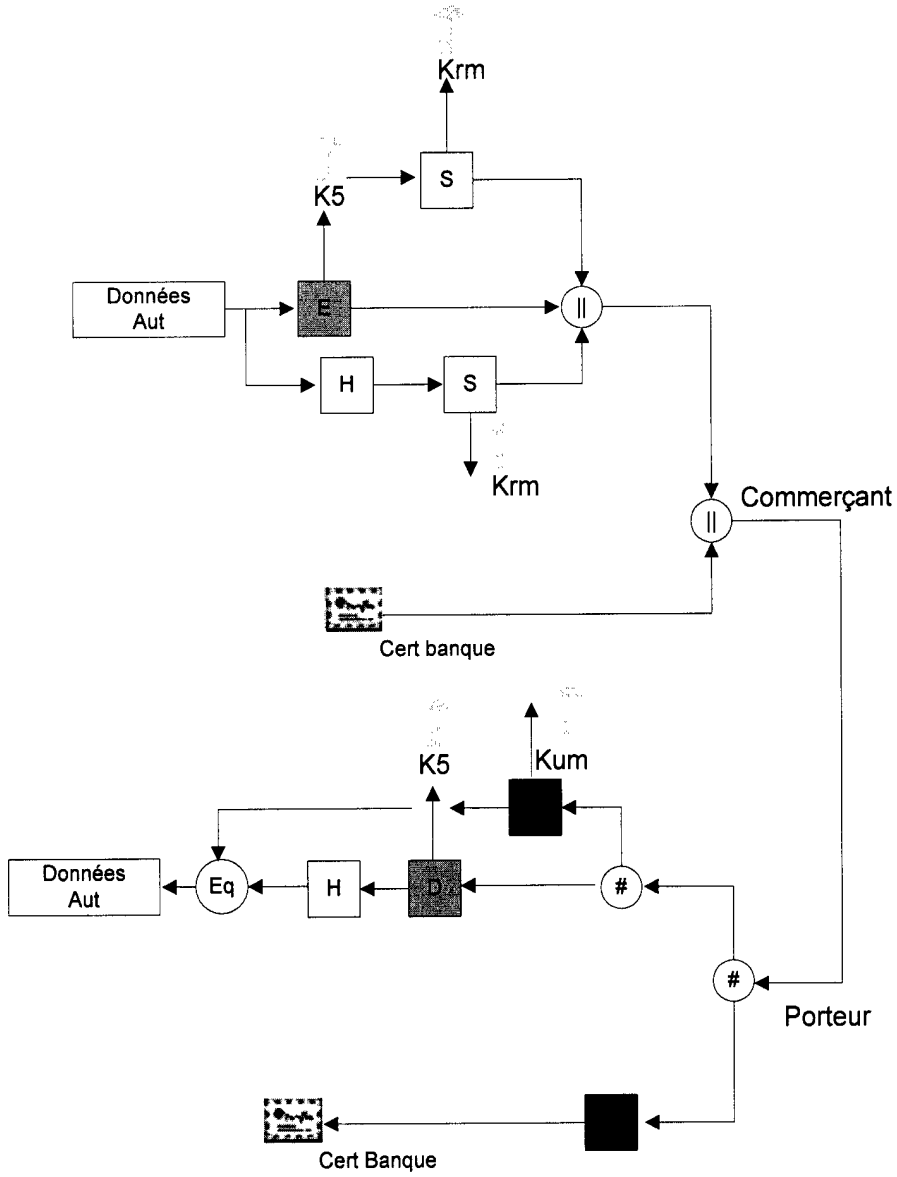
Krm
K5
S
Données Aut
E
II
H
S
Krm
Commerçant
II
Cert banque
K5
Kum
Données Aut
Eq
H
D
#
#
Porteur
Cert Banque

Figure 8

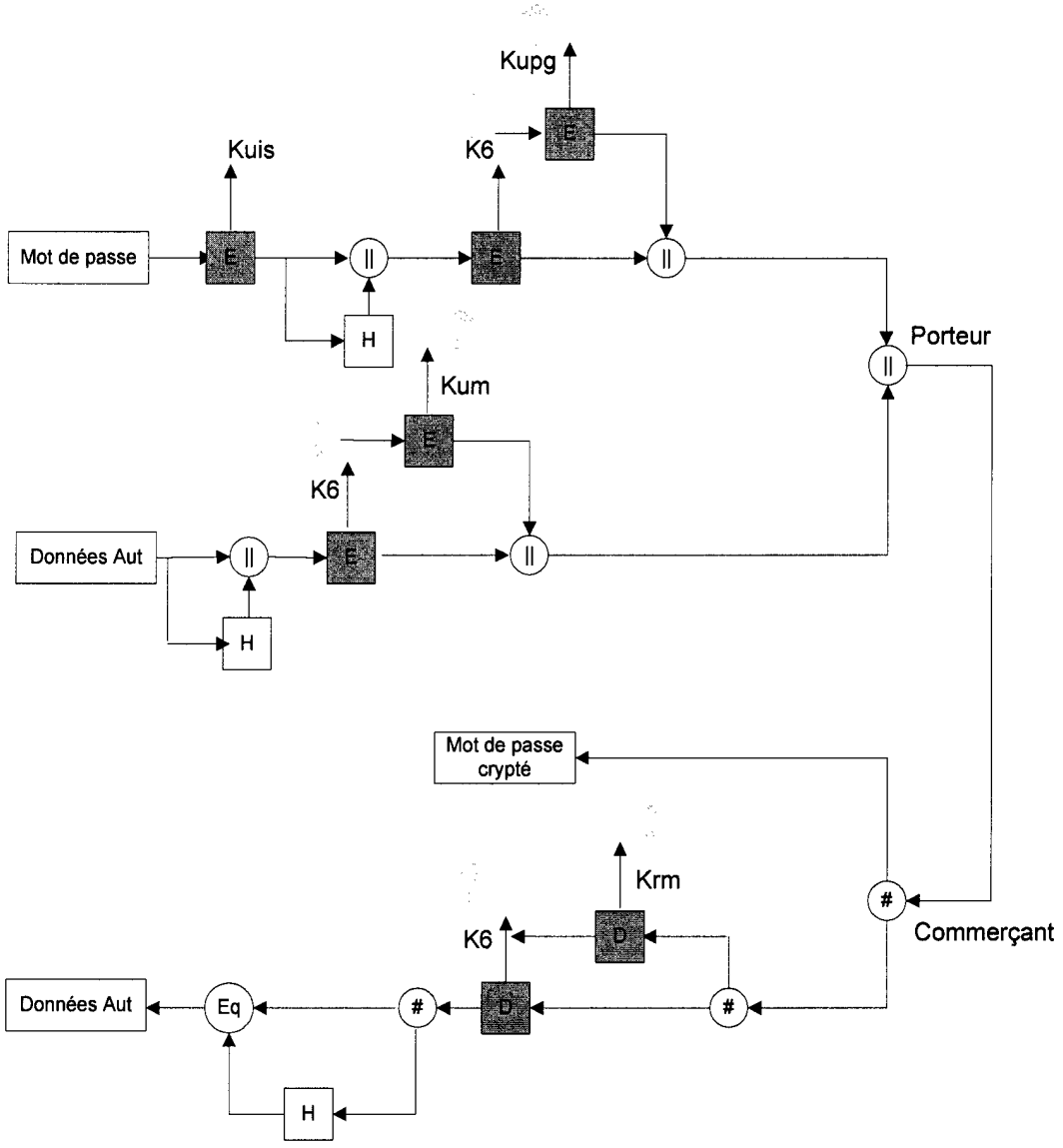
Kupg
Kuis
K6
Mot de passe
E
H
Porteur
Kum
K6
Données Aut
Mot de passe crypté
Krm
Commerçant
Données Aut
Eq
H

Figure 9

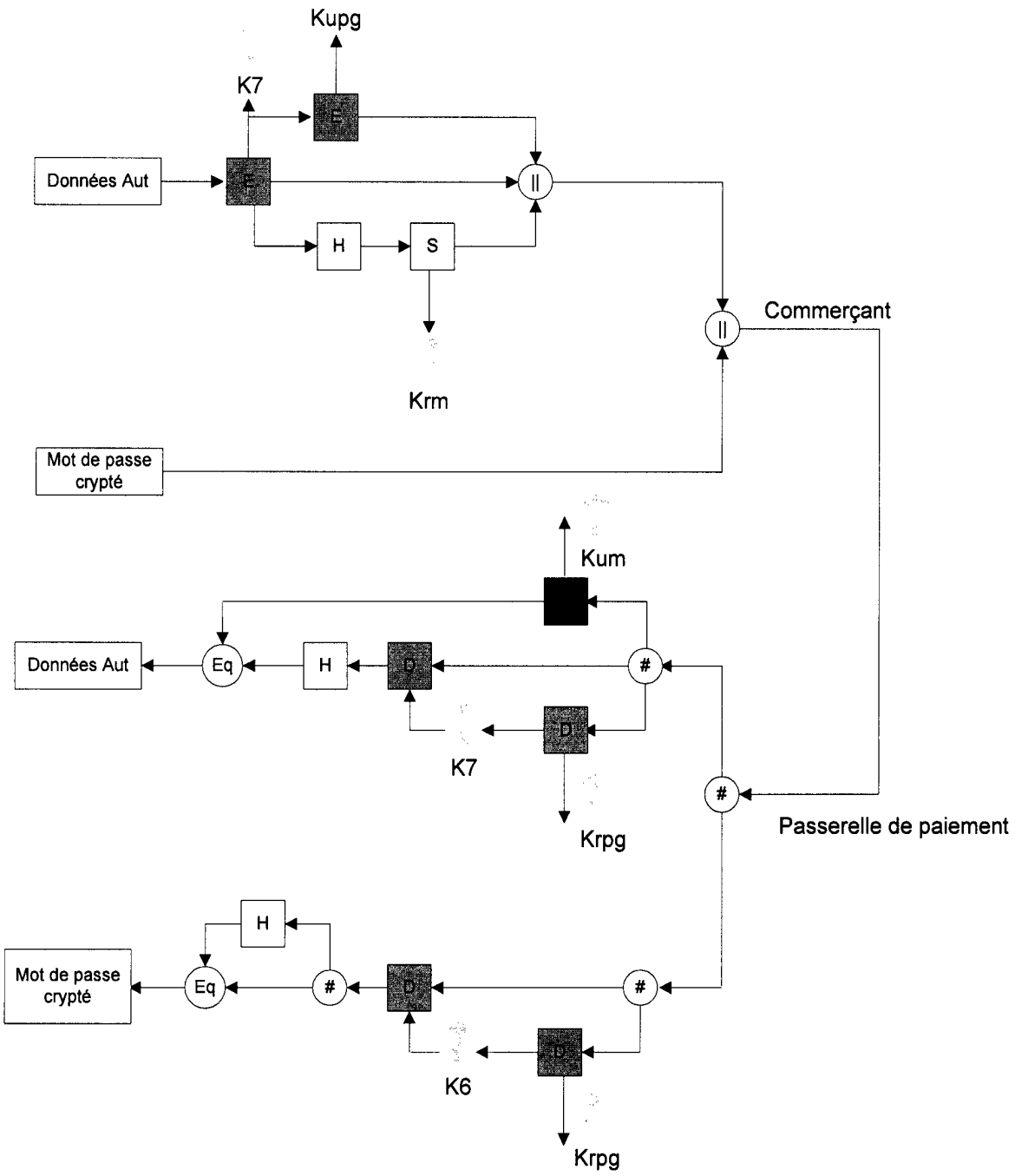
Kupg
K7
E
Données Aut
E
||
H
S
Krm
Commerçant
||
Mot de passe crypté
Kum
Données Aut
Eq
H
D
#
D
K7
Krpg
#
Passerelle de paiement
H
Mot de passe crypté
Eq
#
D
#
D
K6
Krpg

Figure 10

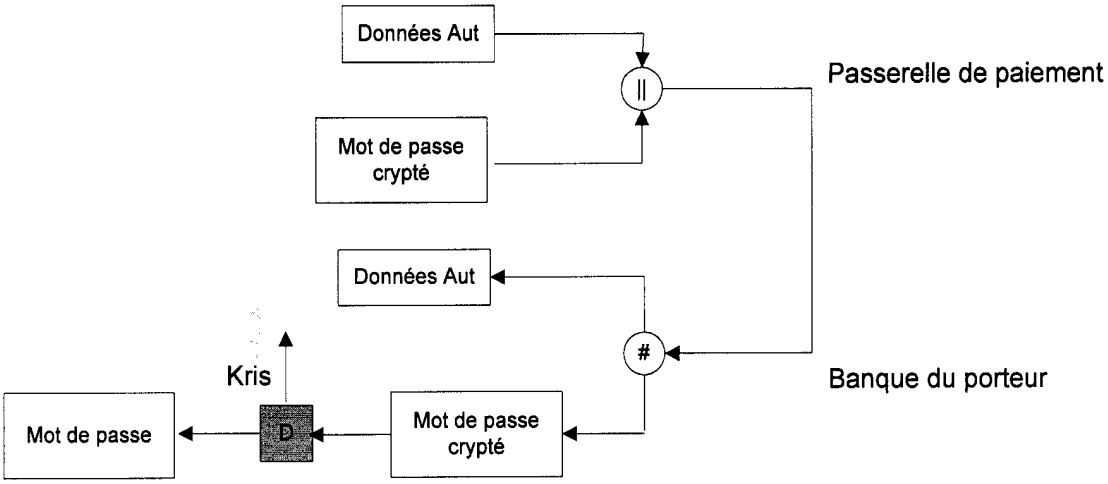

Figure 11

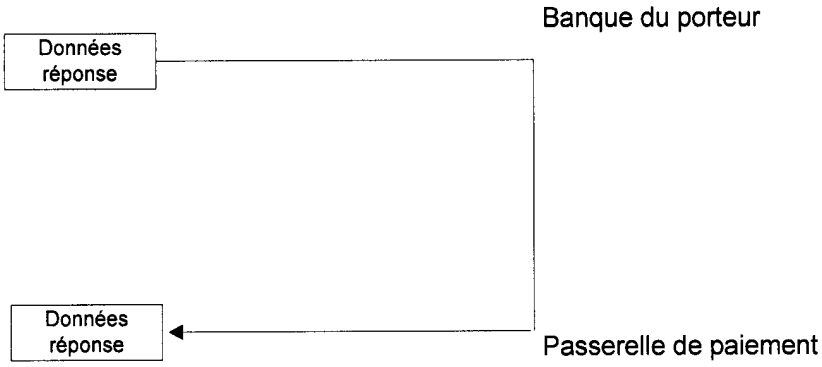

Figure 12

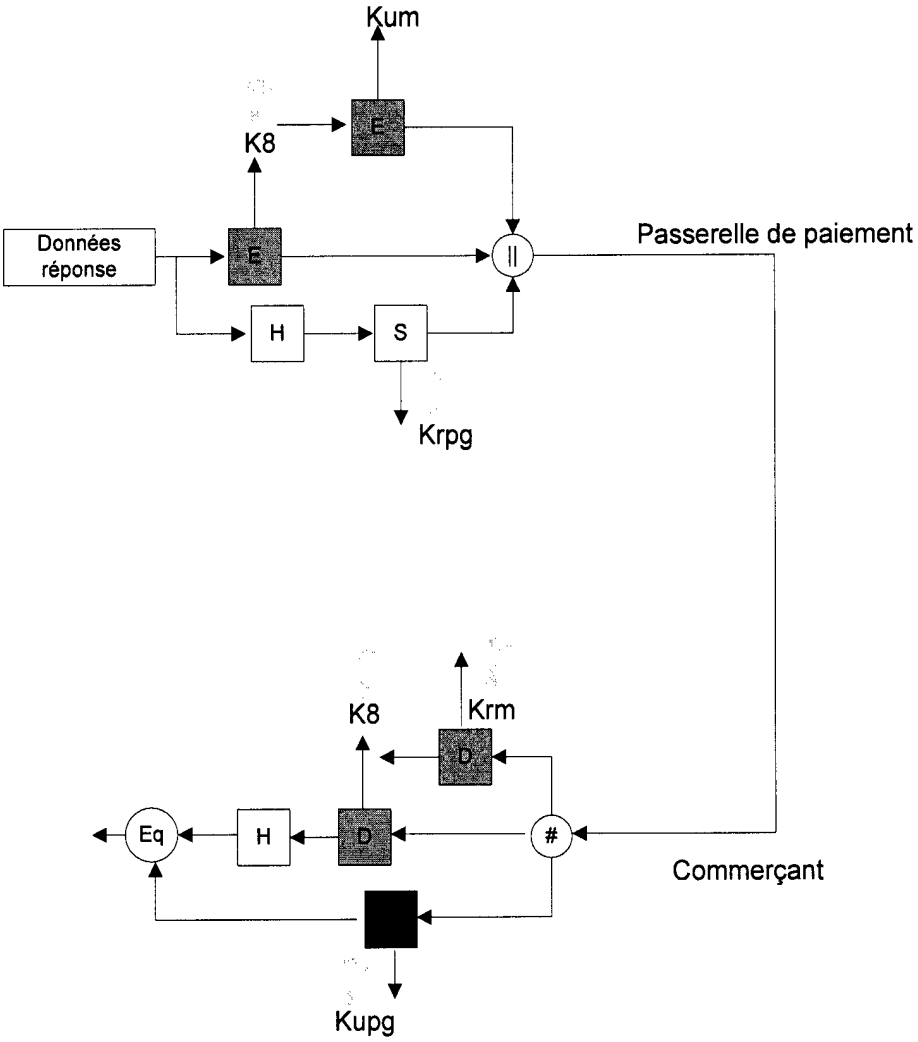
Kum
K8
E
Données réponse
E
||
Passerelle de paiement
H
S
Krpg
K8
Krm
D
Eq
H
D
#
Commerçant
Kupg

Figure 13

MA 37139A1

ROYAUME DU MAROC
OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE

OMPIC

المملكة المغربية
المكتب المغربي للملكية الصناعية والتجارية

RAPPORT DE RECHERCHE AVEC OPINION SUR LA BREVETABILITE

(Conformément aux articles 43 et 43.2 de la loi 17-97 relative à la protection de la propriété industrielle)

Renseignements relatifs à la demande	
N° de la demande : 37139	Date de dépôt : 17/06/2014
Déposant : Université Hassan II Casablanca	Date de Priorité :
Intitulé de l'invention : Conception et implémentation d'un protocole de paiement électronique sécurisé (SEP	

Le présent document est le rapport de recherche avec opinion sur la brevetabilité établi par l'OMPIC conformément aux articles 43 et 43.2, et notifié au déposant conformément à l'article 43.1 de la loi 17-97 relative à la protection de la propriété industrielle telle que modifiée et complétée par la loi 23-13.

Les documents cités par l'examinateur dans la partie rapport de recherche sont joints au présent document

Le présent rapport contient des indications relatives aux éléments suivants :

Partie 1 : Considérations générales
- ☐ Cadre 1 : Base du présent rapport
- ☐ Cadre 2 : Priorité
- ☐ Cadre 3 : Titre et/ou Abrégé tel qu'ils sont définitivement arrêtés

Partie 2 : Rapport de recherche

Partie 3 : Opinion sur la brevetabilité
- ☒ Cadre 4 : Remarques de clarté
- ☒ Cadre 5 : Déclaration motivée quand à la Nouveauté, l'Activité Inventive et l'Application Industrielle
- ☐ Cadre 6 : Observations à propos de certaines revendications dont aucune recherche significative n'a pu être effectuée
- ☐ Cadre 7 : Défaut d'unité d'invention

Examinateur: N KARTIT	**Date d'établissement du rapport** : 25/12/2014
Téléphone: **212 5 22 58 64 14**	
Email : **kartit@ompic.ma**	

MA 37139A1

ROYAUME DU MAROC
****
OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE

OMPIC

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

Partie 1 : Considérations générales

Cadre 1 : base du présent rapport

Les pièces suivantes de la demande servent de base à l'établissement du présent rapport :

- Description
  4 Pages
- Revendications
  6
- Planches de dessin
  9 Pages

Partie 2 : Rapport de recherche

Classement de l'objet de la demande :

CIB : G07F7/08; G07F7/10
CPC :

Bases de données électroniques consultées au cours de la recherche :

EPOQUE, Espacenet, Orbit

Catégorie*	Documents cités avec, le cas échéant, l'indication des passages pertinents	N° des revendications visées
X	http://entreprises.bnpparibas.com/nos-solutions/Gestion-des-flux/Faciliter-vos-encaissements/Cartes/Mercanet/;25/08/2008 BNP Paribas ;	1,3
X	WO2001018720 A1 ; 15 mars 2001 ; Epacific Inc	2
X	WO2001018720 A1 ; 15 mars 2001 ; Epacific Inc	4-6

***Catégories spéciales de documents cités :**

-« **X** » document particulièrement pertinent ; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
-« **Y** » document particulièrement pertinent ; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
-« **A** » document définissant l'état général de la technique, non considéré comme particulièrement pertinent
-« P » documents intercalaires ; Les documents dont la date de publication est située entre la date de dépôt de la demande examinée et la date de priorité revendiquée ou la priorité la plus ancienne s'il y en a plusieurs
-« E » Éventuelles demandes de brevet interférentes. Tout document de brevet ayant une date de dépôt ou de priorité antérieure à la date de dépôt de la demande faisant l'objet de la recherche (et non à la date de priorité), mais publié postérieurement à cette date et dont le contenu constituerait un état de la technique pertinent pour la nouveauté

ROYAUME DU MAROC
OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE

OMPIC

المملكة المغربية
المكتب المغربي للملكية الصناعية والتجارية

Partie 3 : Opinion sur la brevetabilité

Cadre 4 : Remarques de clarté

4.1) Les revendications 1 à 6 doivent comprendre deux parties :

- Un préambule mentionnant la désignation de l'objet de l'invention et les caractéristiques techniques qui sont nécessaires à la définition des éléments revendiqués mais qui, combinées entre elles, font partie de l'état de la technique ;
- Une partie caractérisante, précédée d'une expression du type « caractérisé par », exposant les caractéristiques techniques qui sont celles pour lesquelles la protection est recherchée.

4.2) L'objet représenté dans les figures n'est pas couvert par les revendications. Cette discordance entre les revendications et la description crée un doute quant à l'objet de la protection demandée, au point que les revendications manquent de clarté.

4.3) Les revendications 1 à 6 ont été rédigées en tant que revendications indépendantes distinctes. Conformément à l'art. 7 du décret pour l'application de la loi 17/97, une demande ne peut contenir plus d'une revendication indépendante de même catégorie. Les revendications 2à 6 sont considérées comme des revendications dépendantes.

4.4) Les revendications 1 à 6 sont considérées comme revendications de procédé.

Cadre 5 : Déclaration motivée quand à la Nouveauté, l'Activité Inventive et l'Application Industrielle

Nouveauté (N)	Revendications : 4-6 Revendications : 1-3	Oui Non
Activité inventive (AI)	Revendications : aucune Revendications : 1-6	Oui Non
Possibilité d'application Industrielle (PAI)	Revendications : 1-6 Revendications : aucune	Oui Non

ROYAUME DU MAROC
OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE

OMPIC

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

Il est fait référence aux documents suivants. Les numéros d'ordre qui leur sont attribués ci après seront utilisés dans toute la suite de la procédure

D1 : http://entreprises.bnpparibas.com/nos-solutions/Gestion-des-flux/Faciliter-vos-encaissements/Cartes/Mercanet/
D2 : WO2001018720 A1

1. Nouveauté (N) :

1.1) Le lien http://entreprises.bnpparibas.com/nos-solutions/Gestion-des-flux/Faciliter-vos-encaissements/Cartes/Mercanet/ , présente une solution de paiement sécurisée, pour régler les achats en ligne, elle permet :

- Cryptage avec le protocole SSL (Secure Socket Layer) des informations saisies par le client lors du paiement,
- Transmission des coordonnées bancaires et conservation des données des porteurs sur le serveur de la banque,
- Contrôle les cartes de paiement avec vérification du numéro de la carte, la validité et le cryptogramme,
- Demande d'autorisation de paiement systématique auprès de la banque émettrice à chaque transaction avec rejet immédiat des cartes inexistantes, volées ou perdues,
- Intégration du protocole de sécurisation des transactions 3D Secure : l'internaute porteur d'une carte 3D Secure doit saisir un mot de passe lors du paiement, permettant à sa banque de l'identifier et d'autoriser la transaction (cartes CB, Visa et Mastercard),
- Contrôle de l'encours carte permettant de limiter le nombre de transactions sur une période donnée pour une même carte,
- Possibilité de paramétrer des contrôles anti-fraude supplémentaires.

D'où l'objet des revendications 1 et 3 manque de nouveauté et donc n'implique pas une activité inventive au sens des arts. 26 et 28 de la loi 17/97 modifiée et complétée par la loi 23/13.

ROYAUME DU MAROC
OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE

OMPIC

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

1.2) Le document D1 concerne un procédé et un système (10) d'autorisation d'achats sur un réseau informatique. Un client (12) transmet, sur le réseau (24), un numéro de carte bancaire, à un commerçant en ligne (16) auprès duquel il souhaite effectuer un achat. Le commerçant en ligne (16) envoie ensuite électroniquement le numéro de ladite carte à un contractant tiers (20), par exemple une banque, qui supervise et autorise la transaction. Le contractant tiers (20) détermine par la suite un type de jeton d'authentification associé à la carte et demande au consommateur le jeton d'authentification approprié, En possession du numéro de la carte et du jeton d'authentification, le contractant tiers (20) en vérifie la validité, et contrôle si les fonds sont en suffisance et soit autorise, soit refuse la transaction.

D'où la revendication 2 manque de nouveauté et donc n'implique pas une activité inventive au sens de l'art. 26 de la loi 17/97 modifiée et complétée par la loi 23/13.

1.3) Aucun des documents mentionnés ne divulgue un procédé de paiement en ligne permet de transmettre les données relatives a un achat en deux parties séparément et cryptées sous la clé publique.

D'où l'objet des revendications 4 a 6 est nouveau au sens de l'art. 26 de la loi 17/97 modifiée et complétée par la loi 23/13.

2. Activité inventive (AI) :

Le document D1 est considéré comme l'état de la technique le plus proche de l'objet des revendications 4 à 6, il divulgue un procédé de paiement en ligne sécurisé permettant de transmettre les informations de paiement sur Internet en utilisant une connexion cryptée.

Par conséquent l'objet de ces revendications diffère de ce document par l'envoi des données séparément en deux parties : l'ordre d'achat et l'instruction de paiement.

Il y a aucun effet technique apporté par cette différence.

Le problème objectif que la présente invention se propose de résoudre peut donc être considéré comme la réalisation d'un protocole de paiement sécurisé.

ROYAUME DU MAROC
OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE

OMPIC

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

La solution à ce problème, proposée dans les revendications 4 à 6 de la présente demande, ne peut être considérée comme impliquant une activité inventive pour le motif suivant :

- cette solution est considérée par l'homme du métier comme un développement ordinaire pour résoudre le problème posé.

D'où, l'objet des revendications 4 a 6 n'implique pas une activité inventive au sens de l'art. 28 de la loi 17/97 modifiée et complétée par la loi 23/13.

3. Possibilité d'application industrielle (PAI) :

L'objet de la présente invention est susceptible d'application industrielle au sens de l'article 29 de la loi 17-97 telle que modifiée et complétée par la loi 23-13, parce qu'il présente une utilité déterminée, probante et crédible