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 30987 B1

(51) Cl. internationale :
G06Q 20/00

(43) Date de publication :
01.12.2009

(21) N° Dépôt :
31982

(22) Date de Dépôt :
12.06.2009

(30) Données de Priorité :
16.11.2006 ZA 2006/09533

(86) Données relatives à l'entrée en phase nationale selon le PCT :
PCT/IB2007/054678 16.11.2007

(71) Demandeur(s) :
NET 1 UEPS TECHNOLOGIES, INC., 4TH FLOOR, PRESIDENT'S PLACE, CNR JAN SMUTS AND BOLTON ROAD ROSEBANK, 2196 JOHANNESBURG (ZA)

(72) Inventeur(s) :
BELAMANT, Serge, Christian, Pierre

(74) Mandataire :
ABU-GHAZALEH INTELLECTUAL PROPERTY (TMP AGENTS)

(54) Titre : **TRANSACTIONS FINANCIERES SECURISEES**

(57) Abrégé : UN NUMÉRO DE COMPTE PRINCIPAL (PAN) D'UN COMPTE DE CRÉDIT OU DE DÉBIT CLASSIQUE AVEC UNE BANQUE OU UNE AUTRE INSTITUTION FINANCIÈRE EST ÉMULÉ OU SIMULÉ, ET COMPREND SOUS FORME CRYPTÉE, LE NUMÉRO DE COMPTE RÉEL. LE PAN SIMULÉ PEUT AUSSI COMPRENDRE UN MONTANT À DÉBITER DE CE COMPTE. AINSI, UN NUMÉRO DE COMPTE ET UN MONTANT SONT CRYPTÉS ET MIS EN CORRESPONDANCE DANS UNE CHAÎNE DE CHIFFRES QUI S'AVÈRE ÊTRE UN PAN VALIDE. LE NUMÉRO DE COMPTE RÉEL ET LE MONTANT DE LA TRANSACTION SONT AINSI INTÉGRÉS DANS LE PAN SIMULÉ. LE PAN SIMULÉ EST ENSUITE TRAITÉ PAR L'INFRASTRUCTURE DE TRANSACTION FINANCIÈRE EXISTANTE, LA BANQUE ÉMETTRICE SACHANT QU'IL N'Y A PAS DE PAN, ET QUE LES CHIFFRES CORRECTS DOIVENT ÊTRE CRYPTÉS POUR FOURNIR LE NUMÉRO DE COMPTE INTÉGRÉ ET LE MONTANT INTÉGRÉ. DANS UNE APPLICATION, UN AGENT ÉCONOMIQUE SOUHAITANT EFFECTUER UNE TRANSACTION FINANCIÈRE GÉNÈRE UN PAN SIMULÉ ET LE FOURNIT À UN FOURNISSEUR DE BIENS OU DE SERVICES À QUI IL SOUHAITE

ACHETER CES BIENS OU CES SERVICES. LE FOURNISSEUR ENTRE LE PAN SIMULÉ ET LE MONTANT DE LA TRANSACTION D'UNE MANIÈRE CLASSIQUE. CES DONNÉES SONT ENSUITE TRANSMISES À UNE BANQUE RÉCEPTRICE, QUI LE TRANSMET À LA BANQUE ÉMETTRICE EN VUE D'UNE AUTORISATION. LA BANQUE ÉMETTRICE EXTRAIT ENSUITE LE NUMÉRO DE COMPTE INTÉGRÉ ET LE MONTANT INTÉGRÉ, VÉRIFIE QUE LE MONTANT INTÉGRÉ ET QUE LE MONTANT FOURNI SONT LES MÊMES (AINSI QUE D'AUTRES VÉRIFICATIONS CLASSIQUES), ET SI ILS SONT LES MÊMES ELLE AUTORISE LA TRANSACTION. LES GENS COMPÉTENTS EN MATIÈRE DE FINANCES APPRÉCIERONT CETTE INVENTION, DANS LA PLUPART DES INSTANCES, UN AGENT ÉCONOMIQUE DOIT FOURNIR UNE DATE D'EXPIRATION ET UNE VALEUR DE VÉRIFICATION DE CARTE (CVV). UNE OU LES DEUX FORMALITÉS PEUVENT AUSSI ÊTRE SIMULÉES ET UTILISÉES POUR CRYPTER DES INFORMATIONS.

WO 2008/059465 **PCT/IB2007/054678**

RESUME

Un numéro de compte principal (PAN) d'un compte de crédit ou de débit classique avec une banque ou une autre institution financière est émulé ou simulé, et comprend sous forme cryptée, le numéro de compte réel. Le PAN simulé peut aussi comprendre un montant à débiter de ce compte. Ainsi, un numéro de compte et un montant sont cryptés et mis en correspondance dans une chaîne de chiffres qui s'avère être un PAN valide. Le numéro de compte réel et le montant de la transaction sont ainsi intégrés dans le PAN simulé. Le PAN simulé est ensuite traité par l'infrastructure de transaction financière existante, la banque émettrice sachant qu'il n'y a pas de PAN, et que les chiffres corrects doivent être cryptés pour fournir le numéro de compte intégré et le montant intégré. Dans une application, un agent économique souhaitant effectuer une transaction financière génère un PAN simulé et le fournit à un fournisseur de biens ou de services à qui il souhaite acheter ces biens ou ces services. Le fournisseur entre le PAN simulé et le montant de la transaction d'une manière classique. Ces données sont ensuite transmises à une banque réceptrice, qui le transmet à la banque émettrice en vue d'une autorisation. La banque émettrice extrait ensuite le numéro de compte intégré et le montant intégré, vérifie que le montant intégré et que le montant fourni sont les mêmes (ainsi que d'autres vérifications classiques), et si ils sont les mêmes elle autorise la transaction. Les gens compétents en matière de finances apprécieront cette invention, dans la plupart des instances, un agent économique doit fournir une date d'expiration et une valeur de vérification de carte (CVV). Une ou les deux formalités peuvent aussi être simulées et utilisées pour crypter des informations.

30987 30987

01 DEC 2009

WO 2008/059465 PCT/IB2007/054678

TRANSACTIONS FINANCIERES SECURISEES

Cette invention se rapporte aux transactions financières électroniques. Elle se rapporte plus particulièrement à un générateur de numéro de transaction financière, à un support pour un algorithme pour le générateur, à un module de mémoire pour utilisation avec le générateur, à un système de traitement par une institution financière, à une méthode permettant de réaliser une transaction financière, à une méthode permettant de traiter une transaction financière et à une méthode permettant de faciliter une transaction financière.

Généralement, d'après l'invention, un numéro de compte primaire (« PAN ») d'un compte client ou débiteur conventionnel auprès d'une banque ou autre institution financière est émulé ou simulé, incorporant, sous forme cryptée, le numéro de compte réel. Le PAN simulé peut également incorporer un montant à débiter de ce compte. Ainsi, un numéro de compte et un montant sont cryptés et inscrits dans une chaîne chiffrée apparaissant comme étant un PAN valide. Le numéro de compte réel et le montant de la transaction sont ainsi intégrés dans le PAN simulé. Le PAN simulé est ensuite traité par la structure de transaction financière existante, la banque émettrice sachant qu'il ne s'agit pas d'un PAN et que les chiffres appropriés doivent être décryptés pour obtenir le numéro de compte inscrit et le montant inscrit. Dans une application, une partie à une transaction souhaitant procéder à une transaction financière génère un PAN simulé et le fournit au fournisseur de produits ou de services auprès duquel il souhaite acheter lesdits produits ou services. Le fournisseur saisit le PAN simulé et le montant de la transaction de manière conventionnelle. Ces données sont ensuite transmises à une banque traitant la transaction, qui les transmet à son tour à la banque émettrice pour autorisation. La banque émettrice extrait alors le numéro de compte inscrit et le montant inscrit, vérifie que le montant inscrit et le montant fourni sont les mêmes (en plus des contrôles conventionnels), et s'ils sont les mêmes, autorise la transaction. Les personnes familiarisées avec ces systèmes apprécieront que, dans la plupart des cas, la partie à la transaction doit fournir une date d'expiration et une valeur de vérification de carte (« VVC ») L'une ou l'autre de ces informations peuvent également être simulées et utilisées pour crypter les informations. De plus, les personnes familiarisées avec ces systèmes verront qu'un numéro d'identification bancaire (« NIB ») est fourni dans la première partie du PAN et ce sera toujours le cas avec le PAN simulé.

Par conséquent on pourra apprécier que la sécurité des transactions par Internet et par téléphone en particulier sera améliorée grâce à cette invention.

Ainsi, selon un premier aspect de l'invention, un générateur de numéro de transaction financière est fourni afin de générer un numéro de transaction unique, le numéro de transaction simulant un numéro de compte primaire d'un compte client ou débiteur conventionnel et y incorpore le numéro de compte d'une partie à une transaction.

Le générateur peut également incorporer un montant de transaction dans le numéro de transaction.

De plus, selon ce premier aspect de l'invention, une méthode permettant de procéder à une transaction financière est fournie, incluant la génération d'un PAN simulé contenant un numéro de compte inscrit dans celui-ci, avec éventuellement un montant de transaction.

Cet aspect de l'invention permet encore de fournir ledit PAN simulé à un fournisseur de produits ou de services et la réception dudit PAN simulé par un fournisseur de produits ou de services.

Le PAN simulé peut se présenter sous une forme discernable par l'homme. Il peut se composer en particulier, afin d'opérer avec la structure de transaction existante, d'une chaîne de chiffres numériques. Les personnes familiarisées avec ces systèmes apprécieront le fait que la chaîne peut se composer de 16 à 23 chiffres.

Les personnes familiarisées avec ces systèmes apprécieront également le fait que les 6 premiers chiffres du PAN simulé désigneront le NIB qui, comme expliqué ci-dessus, permet de transférer la transaction à l'institution financière émettrice appropriée, et de permettre à l'institution financière émettrice de reconnaître la réception d'un PAN simulé contenant le numéro de compte et le montant de la transaction inscrits. De la même manière, les personnes familiarisées avec ces systèmes apprécieront que le dernier chiffre du PAN simulé soit un chiffre de vérification.

Le générateur de PAN peut fournir une séquence unique de chiffres représentant les informations cryptées, une nouvelle séquence étant fournie à chaque fois. Le générateur peut ainsi utiliser un algorithme de cryptage approprié afin de fournir une séquence cryptée à chaque fois.

Comme indiqué ci-dessus, la séquence cryptée contient également un montant de transaction.

De plus, comme indiqué ci-dessus, la VVC et/ou la date d'expiration peuvent également être simulées et intégrées aux informations cryptées.

Le générateur peut incorporer un porte-monnaie électronique, le montant de la transaction étant débité lorsque le PAN simulé est généré.

Le PAN simulé peut également disposer, sous forme cryptée, d'une indication de l'identité du bénéficiaire visé. Ainsi, le générateur peut demander à un utilisateur de saisir le nom et le numéro de compte du bénéficiaire visé, qui sont alors également cryptés et inscrits dans le PAN simulé.

Dans le cas où le PAN simulé est destiné à une utilisation par un intermédiaire, il peut être fourni sous une forme cryptée intermédiaire en tant que chaîne alphanumérique, nécessitant un mot de passe à utiliser une seule fois afin de le décrypter et de fournir un PAN simulé utilisable. La forme intermédiaire peut ensuite être envoyée à l'intermédiaire par un canal, le mot de passe par un canal différent. Le générateur peut ensuite disposer d'un dispositif permettant de fournir soit le PAN simulé, soit la forme intermédiaire avec le mont de passe à utilisation unique. De plus, le générateur peut également disposer d'un dispositif permettant de recevoir la forme intermédiaire et le mot de passe, décrypter la chaîne alphanumérique, et fourni un PAN simulé utilisable.

De plus, un moyen de transaction autorisé peut être précisé dans le PAN simulé. Ainsi, si le PAN simulé est uniquement utilisé avec un système au point de vente, au distributeur automatique de billets de banque, avec une transaction téléphonique ou une transaction par Internet, ou l'une d'entre elles, ceci peut également être inscrit dans le PAN simulé.

Le générateur peut inclure un système de traitement électronique, une mémoire, une unité d'entrée pour entrer une demande de PAN simulé et le montant de la transaction, et un écran pour afficher le PAN simulé. On pourra apprécier le fait que le numéro de compte et l'algorithme de cryptage pertinents seront stockés dans la mémoire. Le générateur peut être un dispositif mobile, en particulier un combiné de téléphone portable, auquel cas la mémoire peut être un module d'identification de l'abonné (SIM). On pourra apprécier que, dans le cas où un utilisateur souhaite inclure une indication du bénéficiaire visé, et/ou requiert une chaîne alphanumérique de forme intermédiaire et le mot de passe qui y est associé, et/ou souhaite préciser un mode de transaction particulier, ceci peut être fait via l'unité d'entrée et l'écran, les invites et/ou menus pertinents étant fournis.

Par conséquent, l'invention s'étend à une mémoire telle qu'un SIM dans lequel un NIB, un numéro de compte, un algorithme de cryptage pour crypter le numéro de compte et un montant de transaction fourni pour fournir un PAN simulé incorporant le NIB et une séquence cryptée de chiffres dans laquelle le numéro de compte et le montant de la transaction sont intégrés sont fournis.

L'invention s'étend également à un support permettant de fournir au générateur l'algorithme de cryptage, sur lequel ou dans lequel l'algorithme de cryptage se trouve, de préférence avec le numéro de compte.

L'invention s'étend encore à une méthode permettant de faciliter une transaction financière dans laquelle un numéro de transaction financière crypté simulant un numéro de compte primaire d'une carte de crédit ou de retrait et dans lequel le numéro de compte d'une partie initiant une transaction est incorporé, généré par une partie initiant une transaction, incluant la fourniture à la partie initiant la transaction une mémoire dans laquelle sont stockés le numéro de compte de la partie initiant la transaction et un algorithme de cryptage.

De même, l'invention s'étend également à une méthode permettant de faciliter une transaction financière, dans laquelle un numéro de transaction financière crypté simulant un numéro de compte primaire de carte de crédit ou de retrait conventionnelle, et dans laquelle est incorporée un numéro de compte d'une partie initiant une transaction, est généré par une partie initiant une transaction, qui inclut la transmission à la partie initiant la transaction de son numéro de compte et d'un algorithme de cryptage

De plus, selon un second aspect de l'invention, un système de traitement d'institution financière est fourni afin de traiter un numéro de transaction financière simulant un numéro de compte primaire d'une carte de crédit ou de retrait conventionnelle et dans lequel est incorporé le numéro de compte d'une partie initiant une transaction, qui inclut

un extracteur permettant d'extraire le numéro de compte du numéro de compte primaire simulé.

Cet aspect s'étend à un système permettant de traiter les transactions financières qui inclut un système de traitement d'institution financière tel que décrit ci-dessus, ainsi qu'un générateur de numéro de transaction financière, également comme décrit ci-dessus.

Toujours selon cet aspect de l'invention, une méthode permettant de traiter une transaction financière est fournie, incluant

la réception d'un numéro de transaction financière ostensible qui simule un numéro de compte primaire d'une carte de crédit ou de retrait et dans lequel est incorporé le numéro de compte d'une partie initiant la transaction ainsi qu'une demande d'autorisation du paiement du montant concerné ;

l'extraction du numéro de compte du numéro de compte primaire simulé.

Le PAN simulé peut être reçu via un réseau de communication financière conventionnel.

Comme indiqué ci-dessus, un NIB sera incorporé au PAN, les chiffres restants du PAN simulé étant cryptés. Ainsi, le système peut disposer d'un système de séparation permettant de séparer les chiffres cryptés du NIB. De plus, si le montant de la transaction a également été crypté, le système de décryptage décrypte également le montant de la transaction.

Si, comme discuté ci-dessus, la VVC et/ou la date d'expiration ont également été simulées et contiennent des informations cryptées, elles seront également cryptées.

Si le montant de la transaction est inscrit dans le PAN simulé, le montant inscrit est décrypté et comparé au montant de la transaction fourni de manière conventionnelle, par un système de comparaison. Si les deux montants sont différents, la transaction est refusée.

De même, si le PAN simulé incorpore une indication de la partie à la transaction visée, alors cette information est également extraite et peut être comparée aux coordonnées du bénéficiaire fournies avec le PAN simulé de manière conventionnelle ; et si le PAN simulé incorpore également un mode de transaction spécifié, celui-ci est également extrait et un contrôle peut être réalisé pour vérifier que le mode de transaction utilisé était correct.

Le système peut inclure un système de stockage afin de stocker les PAN simulés qui ont été reçus, ou du moins leurs composants cryptés, et un moyen de comparaison afin de comparer un PAN simulé reçu (ou son composant crypté) avec les PAN simulés stockés (ou leurs composants cryptés) afin de garantir qu'un PAN simulé ne peut être utilisé qu'une seule fois.

Si une transaction est approuvée, une autorisation est envoyée à une banque traitant la transaction ou un fournisseur de produits et de services et le compte approprié de la partie initiant la transaction est débité du montant de la transaction.

L'invention va maintenant être décrite au moyen d'exemples à caractère non limitatif, avec une référence aux schémas qui l'accompagne, dans lesquels :-

La Figure 1 présente une première mise en œuvre de l'invention ;
La Figure 2 présente une deuxième mise en œuvre de l'invention ;
La Figure 3 présente une troisième mise en œuvre de l'invention.

En nous référant à la Figure 1, une première mise en œuvre de l'invention est présentée. Une partie initiant une transaction qui souhaite acheter des produits auprès d'un vendeur dispose d'un générateur sous la forme d'un téléphone portable 10. Le téléphone 10 dispose d'un écran 14, d'un clavier 16 et d'une carte SIM 18. Une application a été chargée sur la carte SIM 18 afin de fournir un PAN simulé tel que discuté ci-dessus. Ainsi, le numéro de compte de la partie initiant la transaction, un NIB, un algorithme de cryptage et un PIN sont stockés sur la carte SIM 18. La partie initiant la transaction saisit, via le clavier 16, une demande d'activation de l'application, ainsi que son PIN, puis saisi le montant de la transaction, en utilisant le clavier 16, lorsque l'écran l'en enjoint. L'application génère alors le PAN simulé, une VVC et une date d'expiration qui sont affichés sur l'écran14. On pourra apprécier que le téléphone 10 et la carte SIM 18 constituent une carte de crédit ou de retrait virtuelle.

La partie initiant la transaction indique le PAN, la VVC et la date d'expiration à un caissier qui saisit manuellement les chiffres fournis sur un dispositif (20) de point de vente (POS) avec le montant concerné. Le PAN simulé est contrôlé par le dispositif au point de vente (20) afin de s'assurer que le chiffre de contrôle est correct et le PAN simulé, la VVC et la date d'expiration, ainsi que le montant de la transaction, sont transmis, de manière conventionnelle, à la banque traitant la transaction 22, via un réseau financier conventionnel 24. La banque traitant la transaction 22 identifie la banque émettrice 26 à partir du NIB et transmet le PAN simulé, la VVC et la date d'expiration, ainsi que le montant de la transaction, à la banque émettrice 26. La banque émettrice 26 dispose d'une interface de communication 28, d'un processus 30

et d'une unité de stockage 32. Le PAN simulé, la VVC et la date d'expiration, ainsi que le montant de la transaction, sont fournis au processeur 30 qui sépare la partie cryptée du PAN simulé, de la VVC et de la date d'expiration. Ceci est ensuite comparé à une liste de toutes les chaînes numériques reçues auparavant et stockées dans l'unité de stockage 32. Si la chaîne est unique et n'a jamais été utilisée auparavant, elle est ajoutée à la liste de chaînes stockées. Si elle a déjà été utilisée et est stockée dans la liste, alors la transaction est refusée et un message à cet effet est envoyé à la banque traitant la transaction 22 puis au vendeur. Si la chaîne n'a jamais été utilisée auparavant, elle est décryptée par le processeur 30 en utilisant un algorithme de décryptage approprié afin d'extraire le numéro de compte de la partie initiant la transaction ainsi que le montant de la transaction inscrit. Aucun PIN ou autre système d'identification n'est requis par la banque émettrice. Le montant de la transaction inscrit est comparé au montant de la transaction fourni, et s'ils diffèrent, la transaction est refusée. Le processeur 30 contrôle que la partie initiant la transaction dispose de suffisamment de fonds, auquel cas le compte de la partie initiant la transaction est débité et une autorisation conventionnelle est fournie à la banque traitant la transaction 22 qui crédite le compte du vendeur et l'informe que la transaction a été effectuée.

La carte SIM 18 peut fonctionner comme un porte-monnaie électronique, auquel cas le porte-monnaie est débité du montant de la transaction lorsque le PAN simulé, la VVC et la date d'expiration sont fournis.

En nous référant à la Figure 2, une deuxième mise en œuvre de l'invention est présentée, dans laquelle une transaction financière est effectuée via l'Internet 40. Dans cette mise en œuvre, le générateur 42 est un ordinateur portable sur lequel l'application est chargée afin de fournir un PAN simulé comme discuté ci-dessus. Le numéro de compte, le NIB, l'algorithme de cryptage et le PIN de la partie initiant la transaction sont également stockés sur l'ordinateur 42.

Lorsque la partie initiant la transaction souhaite acheter des produits ou des services, ou obtenir une pré-autorisation de la part d'un fournisseur, via l'Internet, elle génère un PAN simulé, une VVC et une date d'expiration, qui sont transférés via l'Internet 40 vers un serveur 44 exploité par le fournisseur. Ces informations sont ensuite fournies à la banque traitant la transaction 22 du fournisseur, qui les transfère à la banque émettrice 26. La transaction est ensuite réalisée de manière sécurisée comme décrit ci-dessus en référence à la Figure 1.

De manière similaire, une transaction sécurisée peut être réalisée par téléphone, comme indiqué dans la Figure 3. Dans cette mise en œuvre, le générateur est une fois de plus un téléphone portable 10 comme celui de la Figure 1. Ainsi, la partie initiant la transaction fournit le PAN simulé, la VVC et la date d'expiration tels que fournis par le téléphone 10, via un réseau téléphonique 50 à un opérateur dans un centre d'appels 52. Ces informations sont ensuite transmises avec le montant de la transaction à la banque traitant la transaction 22 et à la banque émettrice 26 de manière conventionnelle. La banque émettrice traite la transaction comme décrit ci-dessus en référence à la Figure 1.

Un exemple de la manière dont le PAN simulé est généré et traité est maintenant fourni.

BIN	PAN	CD	CVV	EXP DATE
6	9	1	3	4
XXXXXX	.....	X	(...)	MM/YY

1. USN client = 3 octets
   1er octet = FI, peut être déterminée par le BIN

   USN = 9876 5432 (8 chiffres max.)

---

2. **Créer la date d'expiration**

- Utiliser 5 années comme date d'expiration de la carte - soit 60 mois, moins 12 mois (pour prendre en compte l'année en cours, moins 1).
- On obtient 48 mois.

EXPDATE= TRXTYPE[2 octets].AID[4 octets]

OU :
AID [2 octets] = 00, 01, 10, 11
TRX TYPE [4 octets] = 0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001, 1010, 1011

MONTH = TRX TYPE + 1 (+1 pour ne pas obtenir month = 0)
MM = Binary_To_ASCII(Month)

YEAR = (année en cours + 1) + AID (CCYY)
YY = Binaire_To_ASCII(les deux derniers chiffres de YEAR)

NOTE :
- MM et YY sont des chiffres affichables (ASCII). Ces 4 chiffres sont saisis en tant que date d'expiration requise sur un terminal
- MONTH[1] = équivalent binaire de MM (le résultat est toujours 1 octet)
- YEAR[2] = équivalent binaire de YEAR y compris de siècle (le résultat est toujours 2 octets)
- AID est le compte/le porte-monnai Débité ou Crédité.

---

3. **Créer les Valeurs d'Application de la Date d'Expiration (EDMV) (Ici, nous avons de la place pour plus de choses)**

- Cette étape introduit un caractère aléatoire dans le mois et l'année créés, ainsi qu'une méthode de vérification que ceci avait été saisi correctement dans le terminal.

EDMV = 1DES((YEAR[2] + 00.MONTH[1])[2].YEAR[2].MONTH[1].(YEAR[2] – 00.MONTH[1])[2].FF)

NOTE :

- Une Clé Statique est utilisée pour créer le bloc crypté (EDMV key)
- Le résultat de (YEAR[2] + 00/MONTH[1]) est toujours une valeur de 2 octets
- Le résultat de (YEAR[2] + 00/MONTH[1]) est toujours une valeur de 2 octets
- EDMV[2] = les 2 derniers octets du résultat EDMV
- EDMV2[2] = les 2 octets en seconde position du résultat EDMV
- Si MM/YY n'ont pas été saisis correctement sur le terminal, alors l'EDMV sera différent et par conséquent, le bloc de cryptage ne sera pas créé correctement et la correspondance avec la CVV échouera.

---

4. Créer un CheckSum pour l'USN – (Clé Diversifiée)

CVV = 3DES(USN[3].ULSN[2].ULP[1].EDMV[2])

NOTE :

- Utilise des DES triples, des clés triples, diversifiés sous USN
- Des clés diversifiées (basées sur USN) sont utilisées pour créer le bloc crypté (Clés Hôtes)
- Convertit la VVC en numéros affichables (ASCII)
- CVV_1 = 3 derniers chiffres du résultat affichable (ASCII).
  Cette valeur à 3 chiffres est saisie en tant que CVV requise sur un terminal (CVV finale)
- CVV_2 = Equivalent binaire de CVV_1 (toujours 2 octets)

---

5. Créer un CheckSum crypté par PIN pour l'USN

- Si les utilisateurs saisissent un PIN, le PIN fera partie de la clé de cryptage.
- Si l'utilisateur ne saisit pas de PIN, un PIN par défaut sera utilisé.

CVV_PIN = 1DES(CVV[8])

NOTE :

- Si AUCUN PIN n'est requis, alors une clé statique (PIN_KEY) est utilisée pour créer le bloc crypté
- Si un PIN est requis, alors le PIN est généré par l'Utilisateur et peut être composé de 4 à 8 chiffres (compris).

Chaque numéro représente un hexadécimal équivalent quartet qui remplacera la PIN_KEY du Quartet le Moins Significatif au Quartet le Plus Significatif

- Convertit le CVV-PIN en chiffres affichables (ASCII)
- CVV_PIN1 = 3 derniers chiffres du résultat affichable (ASCII). Cette valeur à 3 chiffres est saisie en tant que VVC requises sur le terminal
- La CVV est modifiée du fait du PIN et par conséquent, le HOST recréera une CVV incorrecte et la correspondance avec la CVV échouera

---

6. **Créer une Signature de Déchargement**

AMT[2] = 2 derniers octets du Montant de 4 octets
CVV_PIN2[2] = équivalent binaire de CVV_PIN1 (le résultat est toujours 2 octets)

CVV_TEMP = (AMT[2] XOR CVV_PIN2[2])

SIGN = 3DES(AMT[4].CVV_TEMP[2].EDMV2[2])
SIGN = 9999 9999 99

NOTE :

- Les clés statiques sont utilisées pour créer une Signature de déchargement
- La Signature de Déchargement contient généralement un LSN de Déchargement, mais la CVV_TEMPS l'inclut déjà.

7. **SIGN = 8 premiers chiffres**

PAN = USN + SIGN (le résultat est 9 chiffres max). Optionnel - [(USN*YY+YY*MM) + SIGN]
PAN = 9876 5432 (USN) + 9999 9999 (SIGN)
PAN = 1987 6543 1

Calculer le Checksum pour le PAN

- Placer le PAN dans le tampon PAN
- A ce moment, le PAN complet, la Date d'Expiration et la CVV sont créées.

---

8. **Sur Hôte :**

1. Recréer les Valeurs d'Application de la Date d'Expiration (EDMV1 et EDMV2) (Etape 3)
   -LE TRXTYPE et l'AID peuvent être déterminés à partir du MM et de YY
   TRXTYPE[2 octets].AID[3 octets] = ((YY - (année en cours + 1))* 12) + MM

2. Recréer la Signature de Déchargement (SIGN) en utilisant la CVV du terminal (Etapes 4 et 5)
3. USN = PAN-SIGN
4. Maintenant, l'hôte peut obtenir la HOST_KEY, ULSN et ULP
5. Recréer la CVV utilisant l'USN calculée

6. Comparer la CVV recréée (Etape 4) à la CVV transmise par le terminal

Vérifications
1. Correspondance des 3 chiffres de la CVV
2. La CVV n'est pas recréée si la SIGN ne correspond pas
3. La CVV n'est pas recréée si l'USN ne correspond pas
4. La CVV n'est pas appareillée correctement si l'EDSV ne correspond pas.

Résumé Sur la Carte
1. Utiliser l'USN, ULSN, ULP pour créer une CVV
2. Utiliser la CVV pour créer la SIGN
3. Désormais, PAN = USN + SIGN

Résumé sur l'Hôte
1. Utiliser la CVV reçue pour créer la SIGN
2. Utiliser la SIGN pour obtenir l'USN en utilisant le PAN (USN=PAN-SIGN)
3. Utiliser l'USN pour obtenir la HOST KEY, ULSN, ULP pour créer la CVV
4. Comparer la CVV créée à la CVV transmise par le terminal

Les personnes familiarisées avec ces systèmes pourront apprécier qu'il sera extrêmement difficile, si ce n'est impossible, qu'une transaction frauduleuse soit effectuée si la transaction est réalisée conformément à l'invention.

RECLAMATIONS :

1. Un générateur de numéro de transaction financière pour générer un numéro de transaction unique, dans lequel le numéro de transaction simule un numéro de compte primaire de carte de crédit ou de carte de crédit conventionnel et y intègre un numéro de compte d'une partie initiant une transaction.

2. Un générateur de numéro de transaction financière tel que décrit dans la Réclamation 1, dans lequel le numéro de transaction incorpore également un montant de transaction.

3. Un générateur de numéro de transaction financière tel que décrit dans la Réclamation 2, qui inclut une unité d'entrée, opérable par la partie initiant la transaction, par lequel la partie initiant la transaction peut entrer le montant de la transaction.

4. Un générateur de numéro de transaction financière tel que décrit dans la Réclamation 1 ou 2, qui génère une chaîne de chiffres, dont le nombre correspond à un protocole conventionnel, et son numéro prédéterminé initial étant un numéro d'identification bancaire pour identifier une institution financière désignée dans laquelle la transaction sera approuvée et qui sera chargée du paiement du montant de la transaction.

5. Un générateur de numéro de transaction financière tel que décrit dans la Réclamation 3, dans lequel le dernier chiffre de la chaîne est un chiffre de contrôle.

6. Un générateur de numéro de transaction financière tel que décrit dans la Réclamation 1 ou 2, qui génère également une date d'expiration simulée.

7. Un générateur de numéro de transaction financière tel que décrit dans la Réclamation 1 ou 2, qui génère également un numéro de valeur de vérification de carte simulé.

8. Un générateur de numéro de transaction financière tel que décrit dans la Réclamation 1 ou 2, dans lequel le numéro de compte primaire simulé est crypté et qui inclut un système de chiffrement afin de fournir un numéro de compte primaire crypté conformément à un algorithme de cryptage prédéterminé.

9. Un générateur de numéro de transaction financière tel que décrit dans la Réclamation 1, qui incorpore également dans le numéro de compte primaire simulé un identifiant d'un bénéficiaire désigné.

10. Un générateur de numéro de transaction financière tel que décrit dans la Réclamation 1, qui incorpore également un identifiant d'un mode de transaction désigné.

11. Un générateur de numéro de transaction financière tel que décrit dans la Réclamation 2, qui inclut un porte-monnaie électronique, dont le montant du crédit est déduit conformément au montant de la transaction lorsque le numéro de compte primaire simulé est généré.

12. Un générateur de numéro de transaction financière tel que décrit dans la Réclamation 8, qui inclut une mémoire dans laquelle le numéro de compte de la partie initiant la transaction et l'algorithme de cryptage sont stockés.

13. Un générateur de numéro de transaction financière tel que décrit dans la Réclamation 2, qui génère un numéro intermédiaire et un mot de passe qui fournit le numéro de compte primaire simulé lorsqu'un algorithme de décryptage prédéterminé est utilisé.

14. Un générateur de numéro de transaction financière tel que décrit dans la Réclamation 13, qui inclut l'algorithme de décryptage prédéterminé.

15. Un générateur de numéro de transaction financière tel que décrit dans la Réclamation 1, qui est opérable par une partie initiant la transaction.

16. Un support pour fournir un générateur de numéro de transaction financière tel que décrit dans la Réclamation 8 avec l'algorithme de cryptage, dans lequel l'algorithme de cryptage est inscrit.

17. Une mémoire pour utilisation avec un générateur de numéro de transaction financière tel que décrit dans la Réclamation 12, qui inclut le numéro de compte de la partie initiant la transaction et l'algorithme de cryptage.

18. Un système de traitement par une institution financière pour traiter un numéro de transaction financière qui simule un numéro de compte primaire de carte de crédit ou de retrait conventionnel et dans lequel est incorporé un numéro de

compte d'une partie initiant une transaction qui inclut un extracteur pour extraire le numéro de compte du numéro de compte primaire simulé.

19. Un système de traitement par une institution financière tel que décrit dans la Réclamation 18, dans lequel le numéro de la transaction financière incorpore également un montant de transaction et le numéro de transaction financière est reçu avec une demande d'autorisation du paiement d'un montant de transaction, et dans lequel l'extracteur extrait également du numéro de compte primaire simulé le montant de la transaction.

20. Un système de traitement par une institution financière tel que décrit dans la Réclamation 18, qui inclut un système de contrôle à utilisation unique pour s'assurer qu'un numéro de compte primaire simulé reçu ne peut être reçu qu'une seule fois.

21. Un système de traitement par une institution financière tel que décrit dans la Réclamation 20, dans lequel le système de contrôle à utilisation unique inclut un magasin dans lequel au moins des portions désignées de numéros de compte primaire simulés reçus sont stockées et un comparateur pour comparer au moins la portion désignée d'un numéro de compte simulé reçu avec les portions stockées.

22. Un système de traitement par une institution financière tel que décrit dans la Réclamation 19, qui inclut un générateur de message de réponse afin de générer un message à une partie bénéficiaire d'une transaction en vue d'approuver ou de refuser la transaction demandée.

23. Un système de traitement par une institution financière tel que décrit dans la Réclamation 22, qui inclut un système d'envoi pour envoyer le message de réponse à la partie bénéficiaire d'une transaction via un réseau de communication financier conventionnel.

24. Un système de traitement par une institution financière tel que décrit dans la Réclamation 18, qui inclut un système de réception pour recevoir le numéro de compte primaire via n réseau de communication financier conventionnel.

25. Un système de traitement par une institution financière tel que décrit dans la Réclamation 22, qui inclut un système de vérification de la transaction afin de vérifier si la partie initiant la transaction dispose d'un compte, s'il dispose de suffisamment de fonds et si le montant de la transaction prélevé est le même

que le montant de la transaction, et pour autoriser la transaction si ces informations sont toutes correctes, le générateur de message de réponse y étant sensible.

26. Un système de traitement par une institution financière tel que décrit dans la Réclamation 25, qui inclut un système de retrait pour débiter le compte de la partie initiant la transaction du montant de la transaction si la transaction est autorisée.

27. Un système de traitement par une institution financière tel que décrit dans la Réclamation 18, qui inclut un décrypteur afin de décrypter les numéros de compte primaire simulés cryptés.

28. Un système de traitement par une institution financière tel que décrit dans la Réclamation 18, dans laquelle le numéro de transaction financière a été généré par la partie initiant la transaction.

29. Un système pour traiter une transaction financière, qui inclut
un générateur de numéro de transaction financière tel que décrit dans n'importe laquelle des Réclamations 1 à 15 ;
un système de traitement par une institution financière tel que décrit dans n'importe laquelle des Réclamations 18 à 28.

30. Une méthode permettant de réaliser une transaction financière, qui inclut la génération d'un numéro de transaction financière unique qui simule un numéro de compte primaire de carte de crédit ou de retrait conventionnel et y incorpore un numéro de compte d'une partie initiant une transaction.

31. Une méthode permettant de réaliser une transaction financière telle que décrite dans la Réclamation 30, dans laquelle le numéro de transaction financière incorpore le montant d'une transaction.

32. Une méthode permettant de réaliser une transaction financière telle que décrite dans la Réclamation 31, dans laquelle le numéro de transaction financière est généré par la partie initiant la transaction et inclut la saisie du montant de la transaction par la partie initiant la transaction.

33. Une méthode permettant de réaliser une transaction financière telle que décrite dans la Réclamation 30, qui inclut la génération d'une chaîne de chiffres, dont le nombre est conforme à un protocole conventionnel, et son numéro prédéterminé initial étant un numéro d'identification bancaire pour identifier

une institution financière désignée dans laquelle la transaction sera approuvée et qui sera chargée du paiement du montant de la transaction.

34. Une méthode permettant de réaliser une transaction financière telle que décrite dans la Réclamation 33, dans laquelle le dernier chiffre de la chaîne est un chiffre de contrôle.

35. Une méthode permettant de réaliser une transaction financière telle que décrite dans la Réclamation 30, qui inclut également la génération d'une date d'expiration simulée.

36. Une méthode permettant de réaliser une transaction financière telle que décrite dans la Réclamation 30, qui inclut également la génération d'un numéro de valeur de vérification de carte simulé.

37. Une méthode permettant de réaliser une transaction financière telle que décrite dans la Réclamation 30, qui inclut la génération d'un numéro de compte primaire simulé et crypté selon un algorithme de cryptage prédéterminé.

38. Une méthode permettant de réaliser une transaction financière telle que décrite dans la Réclamation 30, qui inclut également l'incorporation dans le numéro de compte primaire simulé l'identifiant d'un bénéficiaire désigné.

39. Une méthode permettant de réaliser une transaction financière telle que décrite dans la Réclamation 30, qui inclut également l'incorporation d'un identifiant d'un système de transaction désigné.

40. Une méthode permettant de réaliser une transaction financière telle que décrite dans la Réclamation 31, qui inclut un porte-monnaie électronique, dont le montant du crédit est déduit conformément au montant de la transaction lorsque le numéro de compte primaire simulé est généré.

41. Une méthode permettant de réaliser une transaction financière telle que décrite à la Réclamation 37, qui inclut la génération d'un numéro intermédiaire et d'un mot de passe qui fournit le numéro de compte primaire simulé requis lorsqu'un algorithme de décryptage prédéterminé est utilisé.

42. Une méthode permettant de réaliser une transaction financière telle que décrite dans la Réclamation 41, qui inclut le décryptage d'un numéro intermédiaire

crypté, au moyen d'un mot de passe et d'un algorithme de décryptage appropriés afin de générer le numéro de compte primaire simulé.

43. Une méthode permettant de réaliser une transaction financière telle que décrite dans la Réclamation 30, dans laquelle le numéro de la transaction financière est généré par la partie initiant la transaction.

44. Une méthode de traitement d'une transaction financière, qui inclut la réception d'un numéro de transaction financière ostensible qui simule un numéro de compte primaire de carte de crédit ou de retrait conventionnelle et dans lequel est incorporé un numéro de compte d'une partie initiant une transaction, ainsi qu'une demande d'autorisation de paiement du montant d'une transaction ;

l'extraction du numéro de compte du numéro de compte primaire simulé.

45. Une méthode de traitement d'une transaction financière telle que décrite dans la Réclamation 44, dans laquelle le numéro de transaction financière reçu incorpore également le montant d'une transaction et inclut également l'extraction du montant de la transaction.

46. Une méthode de traitement d'une transaction financière telle que décrite dans la Réclamation 44, qui inclut de s'assurer qu'un numéro de compte primaire simulé ne peut être utilisé qu'une seule fois.

47. Une méthode de traitement d'une transaction financière telle que décrite dans la Réclamation 46, qui inclut le stockage au moins des portions désignées des numéros de compte primaires simulés reçus auparavant et la comparaison d'au moins la portion désignée d'un numéro de compte primaire simulé reçu aux portions stockées.

48. Une méthode de traitement d'une transaction financière telle que décrite dans la Réclamation 44, qui inclut la génération d'un message de réponse à une partie bénéficiaire d'une transaction à des fins d'approbation ou de rejet de la transaction demandée.

49. Une méthode de traitement d'une transaction financière telle que décrite dans la Réclamation 48, qui inclut l'envoi du message de réponse à la partie bénéficiaire de la transaction via un réseau de communication financier conventionnel.

50. Une méthode de traitement d'une transaction financière telle que décrite dans la Réclamation 44, qui inclut la réception du numéro de compte primaire simulé via un réseau de communication financier conventionnel.

51. Une méthode de traitement d'une transaction financière telle que décrite dans la Réclamation 45, qui inclut de vérifier si la partie initiant la transaction dispose d'un compte, si elle dispose de suffisamment de fonds et si le montant de la transaction prélevé est le même que le montant de la transaction, et l'autorisation de la transaction si ces informations sont correctes.

52. Une méthode de traitement d'une transaction financière telle que décrite dans la Réclamation 51, qui inclut le débit du compte de la partie initiant la transaction du montant de la transaction si la transaction est autorisée.

53. Une méthode de traitement d'une transaction financière telle que décrite dans la Réclamation 44, qui inclut le décryptage des numéros de compte primaires simulés et cryptés.

54. Une méthode de traitement d'une transaction financière telle que décrite dans la Réclamation 44, dans laquelle le numéro de la transaction financière a été généré par la partie initiant la transaction.

55. Une méthode permettant de faciliter une transaction financière dans laquelle un numéro de transaction financière crypté qui simule un numéro de compte primaire de carte de crédit ou de retrait conventionnel et dans lequel est également incorporé un numéro de compte d'une partie initiant une transaction, généré par une partie initiant une transaction, incluant la fourniture à la partie initiant la transaction d'une mémoire dans laquelle sont stockés le numéro de compte de la partie initiant la transaction et un algorithme de cryptage.

56. Une méthode permettant de faciliter une transaction financière dans laquelle un numéro de transaction financière crypté qui simule un numéro de compte primaire de carte de crédit ou de retrait conventionnel et dans lequel est incorporé un numéro de compte d'une partie initiant une transaction, généré par une partie initiant une transaction, qui inclut la transmission à la partie initiant la transaction de son numéro de compte et un algorithme de cryptage.

57. Un générateur de numéro de transaction financière, substantiellement tel que décrit ici en référence aux schémas fournis ici.

58. Un système de traitement par une institution financière, substantiellement tel que décrit ici en référence aux schémas fournis ici.

59. Une méthode permettant d'initier une transaction financière, substantiellement telle que décrite ici en référence aux schémas fournis ici.

60. Une méthode de traitement d'une transaction financière, substantiellement telle que décrite ici en référence aux schémas fournis ici.

WO 2008/059465 PCT/IB2007/054678

WO 2008/059465 PCT/IB2007/054678

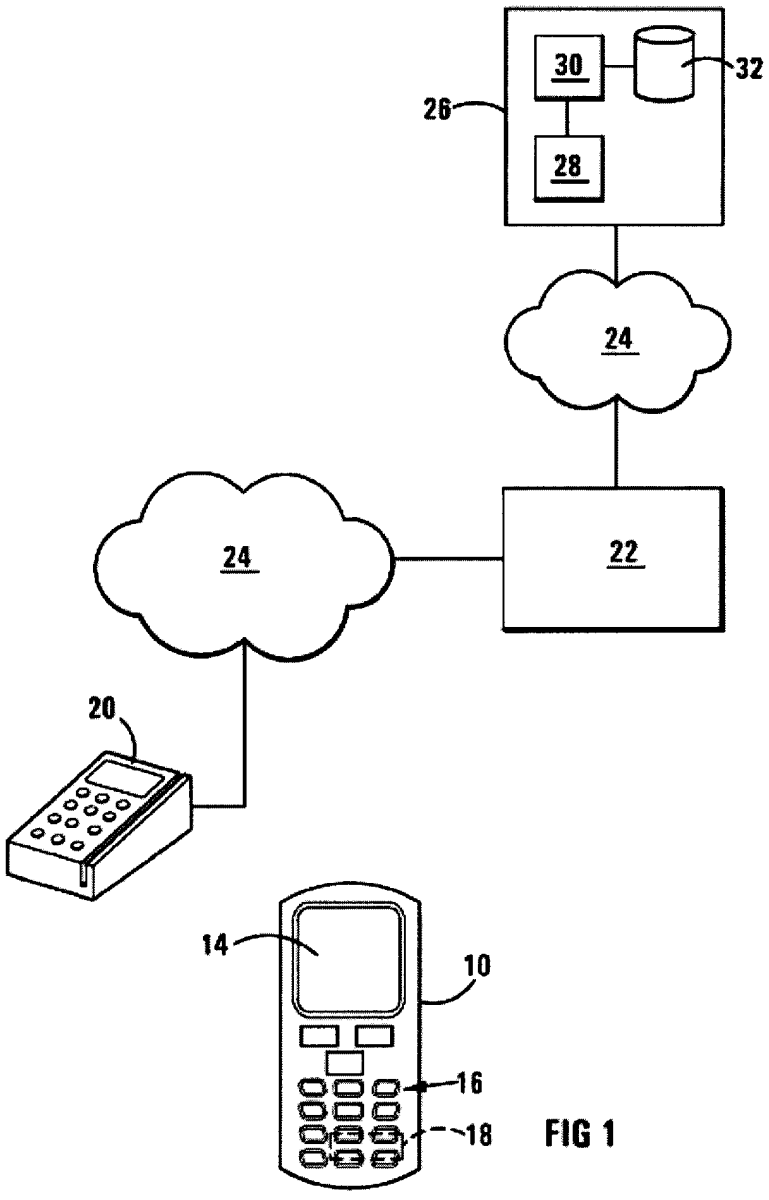

FIG 1

WO 2008/059465 PCT/IB2007/054678

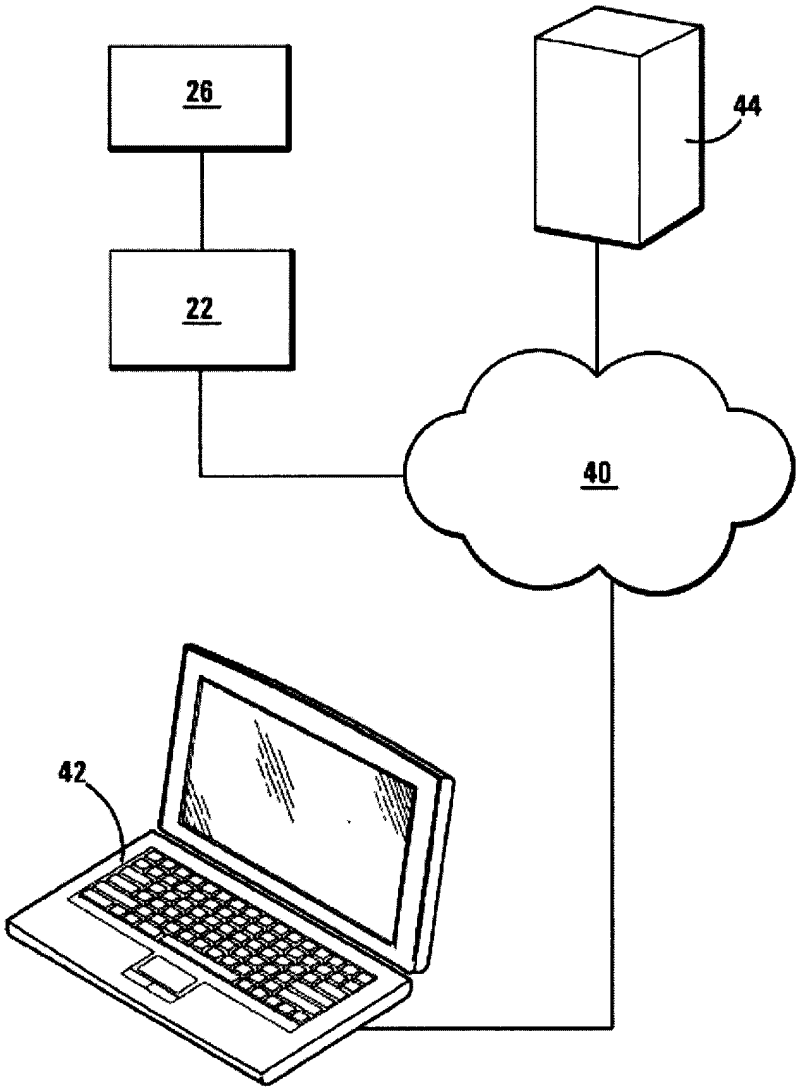

FIG 2

WO 2008/059465 PCT/IB2007/054678

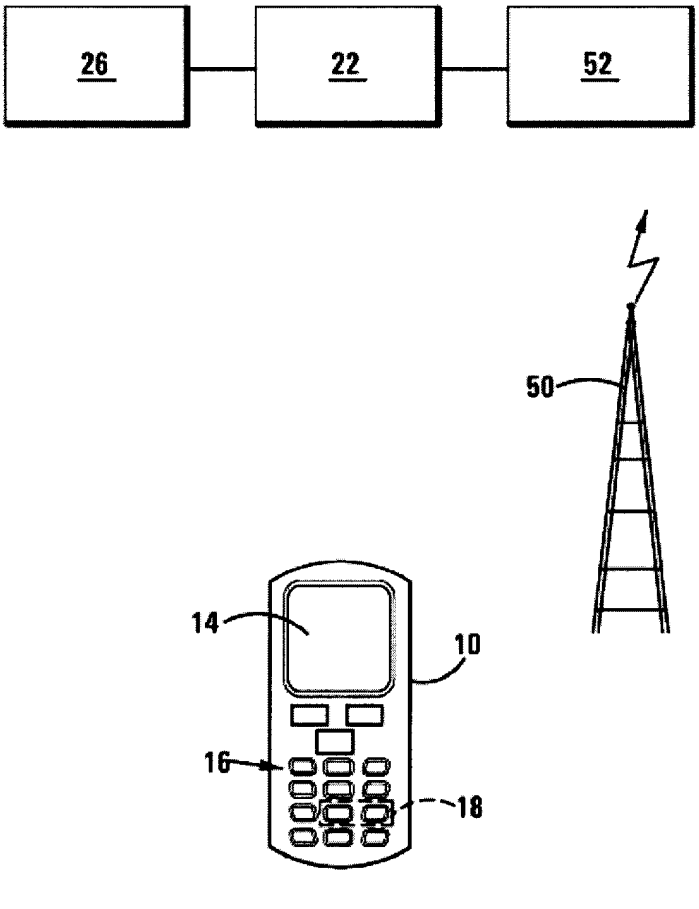

FIG 3