PROCÉDÉ DE TRANSFERT SÉCURISÉ DE DONNÉES PAR UN RÉSEAU DE COMMUNICATION

L'invention concerne les transferts de données réalisés par un réseau de communications. Ce réseau peut par exemple être le réseau téléphonique commuté, le réseau de communication cellulaire tel que le réseau au standard Européen G.S.M ou encore le réseau INTERNET.

Dans le cas des échanges classiques de données entre deux entités, l'authenticité de ces données échangées est garantie par une signature électronique. Cette signature électronique peut être obtenue à l'aide de mécanismes de cryptographie divers tels que des mécanismes de chiffrement, ou d'authentification, ou de signature au sens propre. L'algorithme de calcul correspondant peut être symétrique, auquel cas la clé secrète de signature est partagée par les deux entités, ou asymétrique, auquel cas la clé secrète de signature n'est connue que de l'entité signataire. De tels procédés de transfert de données, permettant l'authentification des données échangées, sont notamment décrits dans la demande de brevet EP - A - 0 683 582 et dans la demande de brevet US 5,534,683.

Aujourd'hui, nous assistons à un fort développement des applications grand public sur des réseaux de communications susceptibles de permettre l'utilisation de cartes à puce. Cependant , l'opération de transfert de données par un réseau est délicate à mettre en oeuvre puisqu'elle peut comporter des échanges entre plusieurs entités et une carte à puce. Les échanges de données par l'intermédiaire d'un réseau peuvent en outre être interrompus pour de multiples raisons telles que, par exemple, la rupture d'une communication,

COPIE DE CONFIRMATION

l'arrachement de la carte à puce ou une panne de l'entité échangeant des données avec la carte à puce. Cette interruption entraîne une désynchronisation des deux entités au détriment de l'une d'entre elles. Les mécanismes connus à ce jour ne permettent pas d'éviter ce problème de désynchronisation en cas d'interruption au cours d'un transfert de données.

La présente invention permet de résoudre ce problème de désynchronisation de deux entités susceptibles d'apparaître lors d'une interruption et propose un procédé de transfert sécurisé de données par un réseau de communications, entre une première entité constituée par une carte à puce et une deuxième entité, apte à garantir l'usage de la carte à puce dans toutes les circonstances même dans le cas d'interruptions au cours de transactions. Ce procédé consiste à élaborer au préalable une signature électronique, permettant de prouver l'initialisation du transfert, et à la stocker dans au moins une zone mémoire de la carte à puce puis, lorsque le transfert est terminé, à effacer cette signature.

Selon une autre caractéristique de l'invention, le procédé comporte une procédure de réclamation, cette procédure consistant à vérifier la présence ou l'absence de la signature dans une zone mémoire de la carte à puce, afin de savoir si le transfert de données a échoué ou abouti.

Selon une autre caractéristique de l'invention, lorsque le transfert de données a été interrompu, la procédure de réclamation consiste en outre à:

- élaborer une nouvelle signature électronique,
- remplacer la signature du transfert échoué par ladite nouvelle signature,

- effectuer les étapes du transfert non encore exécutées, puis
- effacer la nouvelle signature lorsque le transfert est terminé.

Selon une autre caractéristique de l'invention, la signature est stockée de manière sécurisée dans une zone mémoire afin qu'elle ne soit accessible par l'extérieur ni en lecture ni en écriture.

De manière avantageuse, cette zone mémoire est une zone de mémoire électriquement programmable de type EEPROM.

Selon une autre caractéristique de l'invention la signature est élaborée par la deuxième entité et effacée par l'électronique la carte à puce.

Selon une autre caractéristique de l'invention, la signature peut être élaborée au moyen d'un algorithme de cryptographie.

Selon une autre caractéristique de l'invention les données transférées sont des unités de valeur. Dans ce cas la carte à puce peut être un porte-monnaie électronique.

Selon une autre caractéristique de l'invention, le procédé de transfert de données peut être appliqué à une transaction financière entre un organisme bancaire et un porte-monnaie électronique pour créditer le contenu du porte-monnaie, ou entre un fournisseur de services et un porte-monnaie électronique pour débiter le contenu du porte-monnaie.

Selon une autre caractéristique de l'invention, le procédé de transfert de données peut être appliqué à une transaction d'unités de valeurs entre un organisme de jeux et une carte à puce.

La présente invention permet d'éviter des déséquilibres éventuels, susceptibles de se créer entre

deux entités, causés par des interruptions au cours de transferts de données. En effet, la présence de la signature électronique dans une zone mémoire de la carte à puce, après une opération de transfert, indique l'existence d'un déséquilibre et constitue la preuve que l'opération a échoué. Le rétablissement de l'équilibre dans les échanges est réalisé à l'initiative de l'utilisateur de la carte à puce. D'autre part une signature électronique correspondant à un transfert n'est utilisable qu'une seule fois.

D'autres particularités et avantages de l'invention apparaîtront à la lecture de la description faite à titre d'exemple non limitatif en référence aux figures annexées qui représentent:

- la figure 1, un schéma de principe d'un dispositif de mise en oeuvre d'un procédé selon l'invention,
- la figure 2, un organigramme d'un procédé de transfert de données selon l'invention,
- la figure 3, un organigramme d'une procédure de réclamation permettant d'exécuter les étapes du procédé de transfert qui ont été interrompues,
- la figure 4A, un organigramme d'un procédé de transfert appliqué à une transaction financière, entre un organisme bancaire et un porte-monnaie électronique,
- la figure 4B, un organigramme d'une procédure de réclamation permettant l'exécution d'étapes ayant été interrompues au cours de la transaction de la figure 4A,
- la figure 5A, un organigramme d'un procédé de transfert appliqué à une transaction financière entre un porte-monnaie électronique et un fournisseur de services,

- la figure 5B, un organigramme d'une procédure de réclamation permettant l'exécution d'étapes ayant été interrompues au cours de la transaction de la figure 5A.

Le procédé de transfert de données selon l'invention est réalisé entre deux entités dont l'une est de préférence une carte à puce.

La carte à puce utilisée comprend de façon connue un microprocesseur relié par un bus aux différentes mémoires et aux ports d'entrée/sortie de la carte. Parmi les mémoires, il y a en général:

- une mémoire volatile de travail RAM, comme il y en a dans tous les systèmes à microprocesseurs, pour stocker les données intermédiaires nécessaires au cours d'une utilisation de la carte,

- une mémoire morte ROM, contenant des programmes de système permettant le fonctionnement de la carte, programmes qui ne varient pas d'une utilisation à une autre de la carte;

- une mémoire effaçable et programmable électriquement EEPROM, pour l'enregistrement de données destinées à être modifiées et mises à jour au cours des utilisations successives de la carte.

La figure 1 illustre un schéma de principe d'un dispositif de mise en oeuvre d'un procédé de transfert de données selon l'invention. Une carte à puce C est introduite dans la fente d'un organe lecteur enregistreur dénommé dans la suite lecteur L qui peut par exemple être un ordinateur. Le lecteur L est relié, par l'intermédiaire d'un réseau R, à plusieurs entités E1, E2, ...EN susceptibles d'échanger des données avec la carte à puce C.

L'organigramme de la figure 2 illustre les différentes étapes d'un procédé de transfert de données selon l'invention, entre une première entité telle qu'une carte à puce et une deuxième entité E, par l'intermédiaire d'un réseau. Dans une première étape 1, l'entité E élabore une signature électronique pour indiquer l'initialisation du transfert. L'entité commande alors l'écriture de cette signature dans au moins une zone mémoire de la carte à puce, c'est l'étape 2. Cette signature électronique est enregistrée sécuritairement dans cette zone mémoire, c'est-à-dire qu'elle est stockée de manière à ce qu'elle ne soit accessible ni en lecture ni en écriture par l'extérieur. De préférence, la zone mémoire dans laquelle elle est stockée est une zone de mémoire électriquement programmable de type EEPROM.

L'entité E peut en outre posséder des algorithmes de cryptographie de manière à assurer la confidentialité de la signature.

Les étapes suivantes 3, 4 et 5 consistent à effectuer le transfert de données. Pour cela, l'entité commande l'écriture, dans une autre zone de la mémoire EEPROM de la carte à puce, des données caractéristiques du transfert (étape 3). La carte à puce renvoie alors une information d'acquittement selon laquelle elle autorise le transfert (étape 4), puis le transfert est exécuté (étape 5). Lorsque le transfert de données est terminé, le microprocesseur de la carte à puce commande l'effacement de la signature stockée en mémoire (étape 6).

Si une interruption du transfert, due à une rupture de communication, un arrachement intempestif de la carte à puce ou une panne de l'entité E par exemple, se produit entre les étapes 4 et 5 un déséquilibre risque

de se créer au détriment de l'une des deux entités. Grâce au procédé selon l'invention, un tel déséquilibre peut être mis en évidence par la présence de la signature qui n'aura pas été effacée de la mémoire de la carte à puce. La présence de cette signature indique donc une situation d'erreur possible. Le rétablissement de l'équilibre est alors effectué à l'initiative de l'utilisateur de la carte en réalisant une nouvelle connexion entre les deux entités par l'intermédiaire du réseau.

La carte à puce commande alors le déroulement d'une procédure de réclamation dont l'organigramme est représenté sur la figure 3.

Dans un premier temps, à l'étape 4a, l'entité E vérifie la présence ou l'absence de la signature dans la zone mémoire de la carte à puce qui lui est réservée, de manière à vérifier si le transfert de données a échoué ou abouti.

Dans le cas où la signature est présente, c'est à dire lorsque le transfert a échoué, l'entité E élabore alors une nouvelle signature électronique et commande le remplacement de la première signature correspondant au transfert échoué par cette nouvelle signature, c'est l'étape 4b.

Le procédé mis en oeuvre, pour mettre à jour cette signature de manière sécurisée, pourra être par exemple celui qui est décrit dans la demande de brevet FR 95 01791.

L'étape suivante 4c consiste à exécuter les étapes du transfert de données qui ont été interrompues. Enfin, lorsque le transfert de données a été entièrement et correctement exécuté, la nouvelle signature est effacée (étape 4e).

Les données transférées peuvent notamment être des unités de valeurs.

De manière avantageuse, la carte à puce peut être réalisée sous forme de porte-monnaie électronique.

Une application particulière du procédé selon l'invention concerne une transaction financière entre un porte-monnaie électronique (carte C) et un organisme bancaire (entité E1) ou entre un porte-monnaie électronique et un organisme de fourniture de service (entité E2).

Dans ce cas, une unité de valeur correspond, de manière avantageuse, à une unité monétaire.

Une transaction entre un porte-monnaie et un organisme bancaire consiste plus particulièrement à créditer le contenu du porte-monnaie, tandis qu'une transaction entre ce porte-monnaie et un organisme de fourniture de service consiste à le débiter.

La gestion du stockage et de l'effacement de la signature dans la mémoire EEPROM du porte-monnaie électronique dépend du type d'opération effectuée. Elle est en effet différente selon que l'opération consiste à créditer ou à débiter le contenu du porte-monnaie électronique. Cette gestion est expliquée plus en détail dans ce qui suit.

L'organigramme de la figure 4A illustre le chargement d'un porte-monnaie électronique au cours d'une transaction financière avec un organisme bancaire.

Dans l'exemple représenté sur cette figure, préalablement à l'initialisation de la transaction, le contenu du porte-monnaie comporte 5 unités de valeur UV, et le compte bancaire de l'utilisateur du porte-monnaie comporte 500 UV.

Lorsqu'un utilisateur demande le chargement de son porte-monnaie d'une valeur de 100 unités de valeurs UV par exemple (étape 10), la banque, après avoir vérifié le solde du compte utilisateur, construit une preuve de la transaction, c'est-à-dire qu'elle calcule une signature électronique, et la transmet au porte-monnaie (étape 20).

Le porte-monnaie stocke la signature électronique et les données caractéristiques de la transaction dans une zone de mémoire EEPROM et renvoie à la banque une information d'acquittement autorisant l'exécution de la transaction (étape 30).

La banque débite alors le compte utilisateur et ordonne le chargement correspondant du porte-monnaie (étape 40). Le crédit est effectué et, simultanément, le porte-monnaie efface la signature en mettant en oeuvre le procédé de mise à jour sécurisée de mémoire EEPROM décrit dans la demande de brevet FR 95 01791.

Lorsque l'opération de transaction est terminée, le contenu du porte-monnaie électronique doit par conséquent être égal à 105 UV, tandis que le contenu du compte bancaire de l'utilisateur du porte-monnaie est égal à 400 UV.

Une interruption entre les étapes 30 et 40 peut entraîner un déséquilibre entre le porte-monnaie et la banque au détriment de l'utilisateur. En effet, il se peut que le compte bancaire de l'utilisateur ait été débité alors que son porte-monnaie n'a pas été crédité.

Cependant, lorsqu'une telle interruption se produit, le chargement du porte-monnaie n'ayant pas abouti, la signature n'est pas effacée de la mémoire EEPROM du porte-monnaie. La présence de cette signature permet donc de prouver que la transaction a échoué. L'utilisateur doit alors reconnecter son porte-monnaie

à l'organisme bancaire, par l'intermédiaire du réseau, pour rétablir l'équilibre.

Lors de la reconnexion, le microprocesseur du porte-monnaie électronique lance le déroulement d'une procédure de réclamation, dont l'organigramme est illustré sur la figure 4B.

Dans l'exemple de la figure 4B, le compte bancaire de l'utilisateur a été débité de 100 UV et est égal à 400 UV, alors que le contenu du porte monnaie n'a pas été crédité et est resté égal à 5 UV.

Lors de la réclamation, le porte-monnaie présente donc à la banque les données caractéristiques de la transaction et la preuve que cette transaction a été interrompue, c'est-à-dire la signature électronique (étape 31). La banque vérifie cette signature électronique et valide la procédure de réclamation. Puis elle construit une nouvelle preuve de la transaction et la transmet au porte-monnaie (étape 32).

Le porte-monnaie stocke alors la nouvelle signature électronique, en remplacement de celle correspondant à l'opération de crédit échouée, et les données caractéristiques de la nouvelle transaction, puis envoie à la banque une information d'acquittement autorisant la transaction (étape 33). Le remplacement de la première signature électronique correspondant à la transaction interrompue par la nouvelle signature électronique est réalisé au moyen du procédé de mise à jour sécurisée de mémoire EEPROM décrit dans la demande de brevet FR 95 01791.

Si le compte bancaire de l'utilisateur n'a pas été débité lors de la première transaction, la banque effectue le débit puis, dans tous les cas, elle ordonne le chargement du porte-monnaie, c'est l'étape 34.

Dans l'exemple de la figure 4B, le compte bancaire a été débité avant l'interruption de la première transaction. Dans ce cas, la banque ordonne le chargement du contenu du porte-monnaie juste après avoir reçu l'information d'acquittement autorisant la transaction.

Le porte-monnaie efface la nouvelle signature de la transaction simultanément à l'opération de crédit (étape 35).

De la même manière, une transaction financière peut avoir lieu entre un porte-monnaie électronique et un fournisseur de services. Dans ce cas, le fournisseur de services, en échange d'un service à rendre, commande le débit d'une certaine valeur du contenu du porte-monnaie. Cette transaction entre porte-monnaie et fournisseur de services est représentée sur la figure 5A.

Lorsqu'un utilisateur demande un service (étape 100), le fournisseur de services élabore une preuve de la commande, c'est-à-dire une signature électronique correspondant à la transaction à effectuer.

Le porte-monnaie est ensuite débité de la valeur correspondant au service, 5 UV dans l'exemple de la figure 5A, et la signature et les données caractéristiques de la transaction sont simultanément enregistrées dans la mémoire EEPROM du porte-monnaie, c'est l'étape 200.

Le porte-monnaie émet alors des certificats de débit et les transmet au fournisseur (étape 300). Le fournisseur vérifie ces certificats, les enregistre et acquitte le paiement (étape 400). Le paiement ayant été acquitté, la signature électronique correspondant à la commande est effacée de la mémoire EEPROM du porte-monnaie électronique (étape 500).

S'il y a une coupure entre les étapes 300 et 400, la présence de la signature dans la mémoire EEPROM du porte-monnaie témoigne d'une situation d'erreur possible. Cette situation d'erreur peut par exemple correspondre au fait que le paiement n'a pas été encaissé par le fournisseur alors que le contenu du porte-monnaie a été débité. Or, tant que le fournisseur n'est pas payé, il ne fournit pas le service requis correspondant. Pour obtenir le service qu'il a payé, l'utilisateur doit en conséquence présenter la preuve de la commande, c'est-à-dire la signature électronique correspondant à la transaction demandée, et éventuellement renvoyer les certificats de paiement s'ils n'ont pas été reçus par le fournisseur.

L'organigramme de la figure 5B décrit le déroulement de la procédure de réclamation permettant d'achever le paiement d'un fournisseur de services.

Dans l'exemple de cette figure 5B, le contenu du porte-monnaie a été débité de 5UV, lors de la première transaction correspondant à la figure 5A, alors que le paiement n'a pas été encaissé par le fournisseur, le contenu de la caisse étant resté égal à 500 UV. Le porte-monnaie transmet dans un premier temps au fournisseur les éléments de la réclamation, c'est-à-dire les données caractéristiques de la transaction échouée et la signature.

Dans le cas où le(s) certificat(s) a(ont) été reçu(s) par le fournisseur, ce dernier acquitte le paiement et la preuve de la transaction est effacée (étapes 340-350).

En revanche, dans le cas où le(s) certificat(s) n'a(ont) pas été reçu(s) par le fournisseur, celui-ci vérifie la validité de la réclamation, c'est-à-dire la présence de la signature électronique. Il élabore par

ailleurs une nouvelle signature électronique qu'il transmet au porte-monnaie accompagnée d'une demande de paiement, c'est-à-dire d'une demande du (des) certificat(s) (étape 320).

Le porte-monnaie enregistre les données caractéristiques de la transaction dans la mémoire EEPROM ainsi que la nouvelle signature électronique en remplacement de la précédente, et il recalcule les certificats du débit échoué (étape 330).

Les certificats reçus, enregistrés et vérifiés, le fournisseur acquitte le paiement (étape 340). Enfin, le porte-monnaie efface la preuve de la transaction (étape 350).

La procédure de réclamation terminée, le contenu du porte-monnaie est débité, le fournisseur a encaissé le paiement et peut donc rendre le service correspondant requis par l'utilisateur du porte-monnaie électronique.

Les exemples qui viennent d'être décrits permettent de comprendre en quoi la gestion du stockage et de l'effacement de la signature est différent selon le type d'opération effectuée.

Ainsi, dans le cas d'un crédit, l'effacement de la signature et le crédit du contenu du porte-monnaie se font simultanément.

En revanche, dans le cas d'un débit, c'est l'enregistrement de la signature et le débit du contenu du porte-monnaie qui se font simultanément.

Selon une autre variante de réalisation, le procédé de transfert de données selon l'invention peut également être appliqué à une transaction d'unités de valeurs entre un organisme de jeux et une carte à puce par l'intermédiaire d'un réseau.

Dans ce cas les données transférées sont des unités de valeurs correspondant chacune à une somme d'argent

définie au préalable. Le rechargement du contenu de la carte à puce est réalisé au moyen d'une banque interne à l'organisme de jeux. Par ailleurs, le contenu de la carte à puce est crédité ou débité selon que l'utilisateur a gagné ou perdu un jeu. Les transactions effectuées sont donc semblables aux transactions financières qui viennent d'être décrites.

Une signature électronique, destinée à prouver qu'une transaction a échoué, n'est utilisable qu'une seule fois: la signature d'une transaction échouée est remplacée par une nouvelle signature électronique de transaction de réclamation et, dans tous les cas, la signature est effacée lorsque la transaction a abouti.



REVENDICATIONS

1. Procédé de transfert sécurisé de données par un réseau de communications, entre une première entité constituée par une carte à puce et une deuxième entité,
consistant à élaborer au préalable une signature électronique, celle-ci permettant de prouver l'initialisation du transfert, et à la stocker dans au moins une zone mémoire de la carte à puce puis, lorsque le transfert de données est terminé, à effacer cette signature, ledit procédé comportant une procédure de réclamation, cette procédure consistant à vérifier la présence ou l'absence de la signature électronique dans une zone mémoire de la carte à puce, afin de savoir si le transfert de données à échouer ou abouti, caractérisé en ce que, lorsque le transfert de données a été interrompu, la procédure de réclamation consiste en outre à:

- élaborer une nouvelle signature électronique,
- remplacer la signature du transfert échoué par ladite nouvelle signature,
- effectuer les étapes du transfert non encore exécutées, puis
- effacer la nouvelle signature lorsque le transfert est terminé.

2. Procédé selon la revendication 1 caractérisé en ce que la signature est stockée de manière sécurisée dans une zone mémoire afin qu'elle ne soit accessible par l'extérieur ni en lecture ni en écriture.

3. Procédé selon l'une des revendications 1 à 2, caractérisé en ce que la zone mémoire de la carte à puce dans laquelle est stockée la signature est une zone de mémoire électriquement programmable de type EEPROM.

4. Procédé selon l'un des revendications 1 à 3, caractérisé en ce que la signature électronique est élaborée par une deuxième entité et effacée par l'électronique de la puce.

5. Procédé selon l'une des revendications 1 à 4, caractérisé en ce que la signature électronique est élaborée au moyen d'un algorithme de cryptographie.

6. Procédé selon l'une des revendications 1 à 5, caractérisé en ce que les données transférées sont des unités de valeurs.

7. Procédé selon l'une des revendications 1 à 6, caractérisé en ce que la carte à puce est un porte-monnaie électronique.

8. Application du procédé selon l'une des revendications 1 à 7 à une transaction financière entre un organisme bancaire et un porte-monnaie électronique pour créditer le contenu de ce dernier, ou entre un fournisseur de services et un porte-monnaie électronique pour débiter le contenu de ce dernier.

9. Application selon la revendication 8 caractérisée en ce que le cas où le contenu du porte-monnaie est crédité, l'opération de crédit et l'effacement de la signature se font simultanément.

10. Application selon la revendication 8 caractérisée en ce que dans le cas où le contenu du porte-monnaie est débité, le stockage de la signature dans une zone mémoire et l'opération de débit se font simultanément.

11. Application du procédé selon l'une des revendications 1 à 7 à une transaction d'unités de valeurs entre un organisme de jeux et une carte à puce.

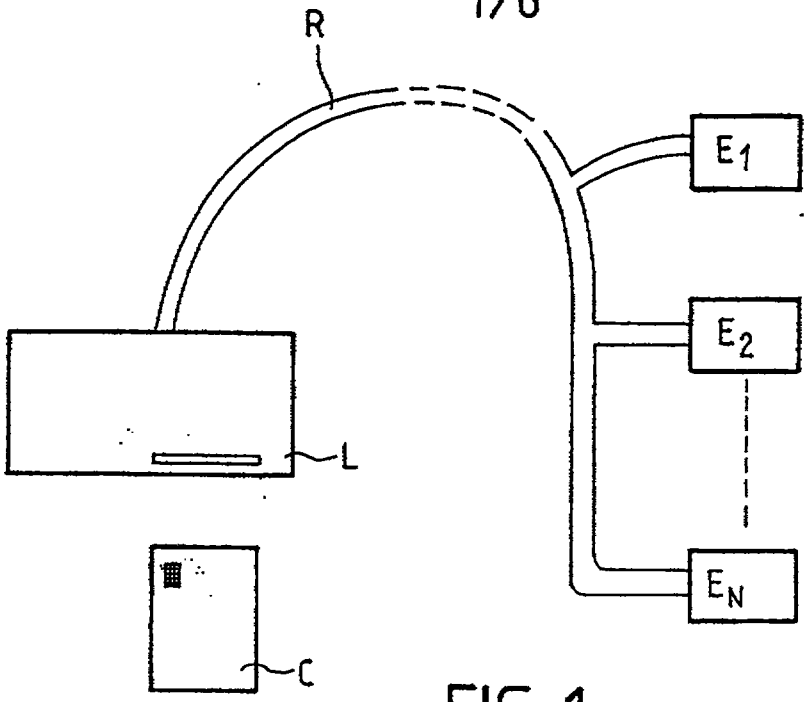
R
E1
E2
EN
L
C

FIG_1

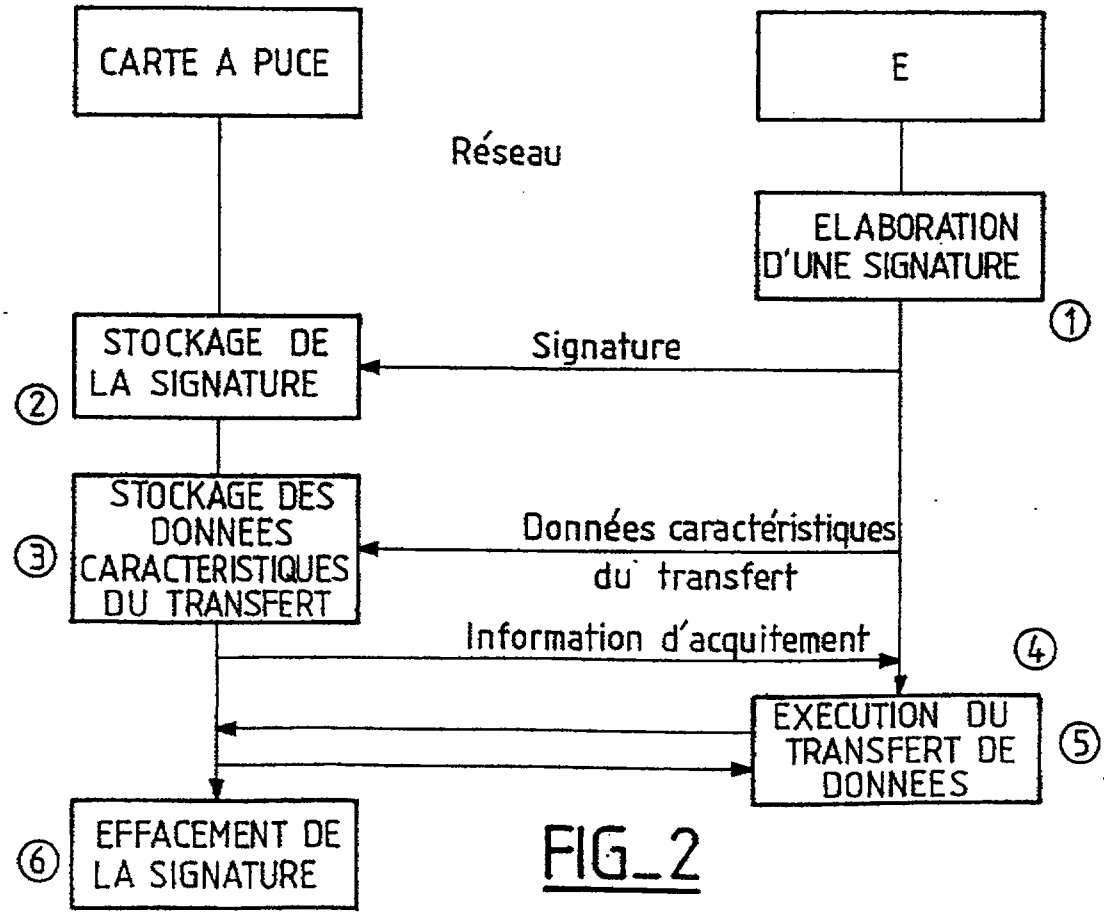
CARTE A PUCE
E
Réseau
ELABORATION D'UNE SIGNATURE
1
STOCKAGE DE LA SIGNATURE
2
Signature
STOCKAGE DES DONNEES CARACTERISTIQUES DU TRANSFERT
3
Données caractéristiques du transfert
Information d'acquitement
4
EXECUTION DU TRANSFERT DE DONNEES
5
EFFACEMENT DE LA SIGNATURE
6

FIG_2

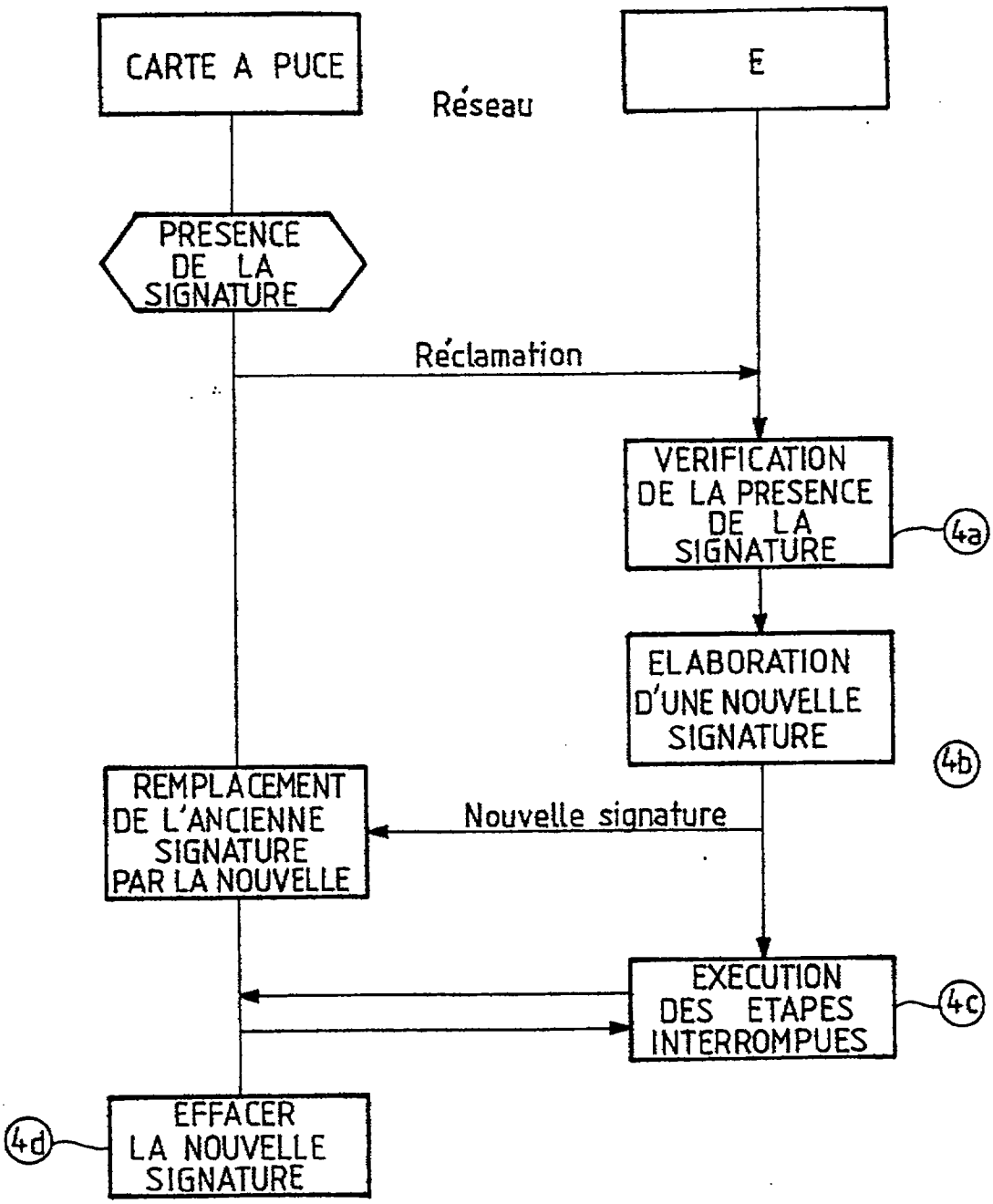
CARTE A PUCE
Réseau
E
PRESENCE DE LA SIGNATURE
Réclamation
VERIFICATION DE LA PRESENCE DE LA SIGNATURE
4a
ELABORATION D'UNE NOUVELLE SIGNATURE
4b
REMPLACEMENT DE L'ANCIENNE SIGNATURE PAR LA NOUVELLE
Nouvelle signature
EXECUTION DES ETAPES INTERROMPUES
4c
EFFACER LA NOUVELLE SIGNATURE
4d

FIG_3

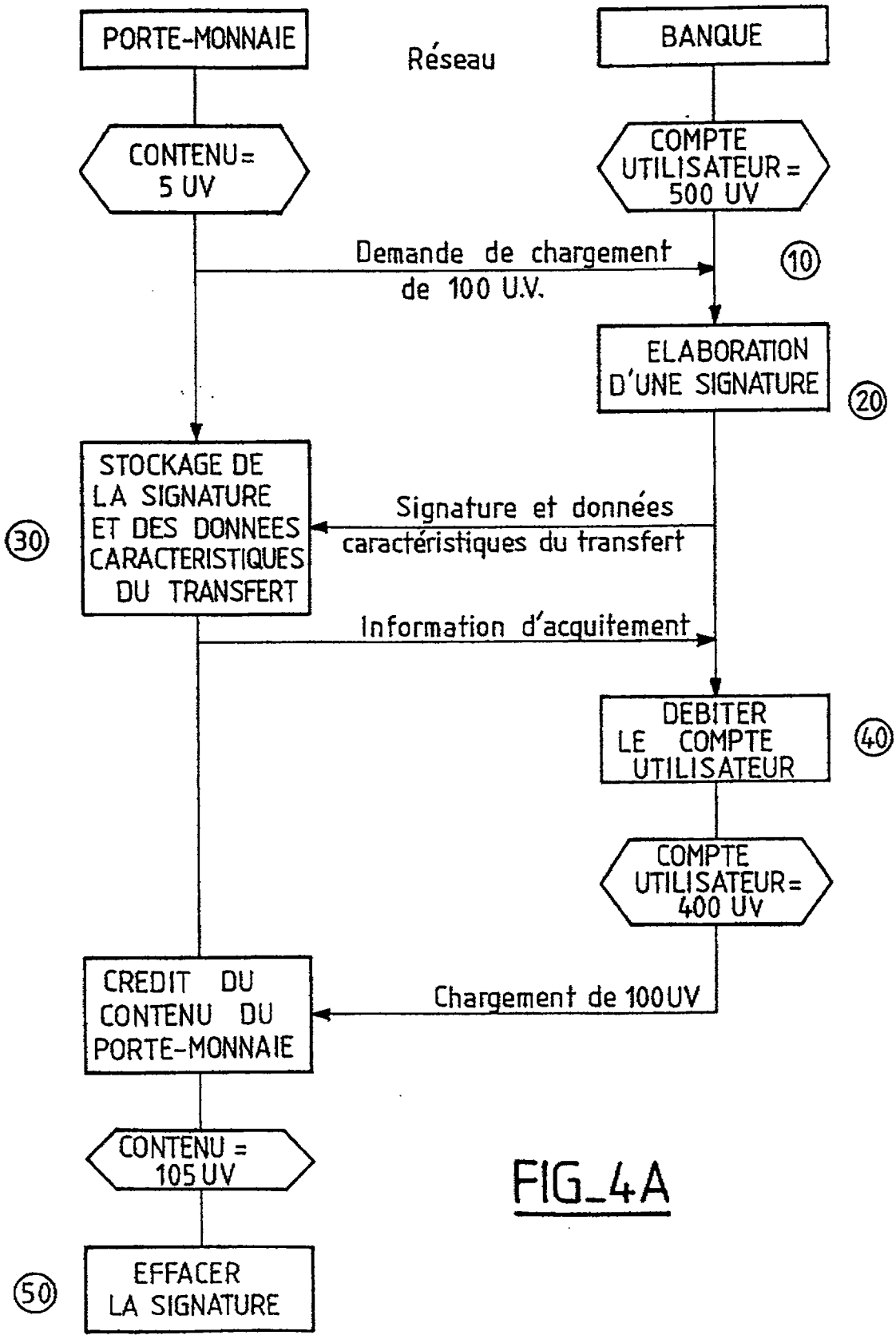
PORTE-MONNAIE
Réseau
BANQUE
CONTENU= 5 UV
COMPTE UTILISATEUR = 500 UV
Demande de chargement de 100 U.V.
10
ELABORATION D'UNE SIGNATURE
20
STOCKAGE DE LA SIGNATURE ET DES DONNEES CARACTERISTIQUES DU TRANSFERT
30
Signature et données caractéristiques du transfert
Information d'acquitement
DEBITER LE COMPTE UTILISATEUR
40
COMPTE UTILISATEUR= 400 UV
CREDIT DU CONTENU DU PORTE-MONNAIE
Chargement de 100UV
CONTENU = 105 UV
EFFACER LA SIGNATURE
50

FIG_4A

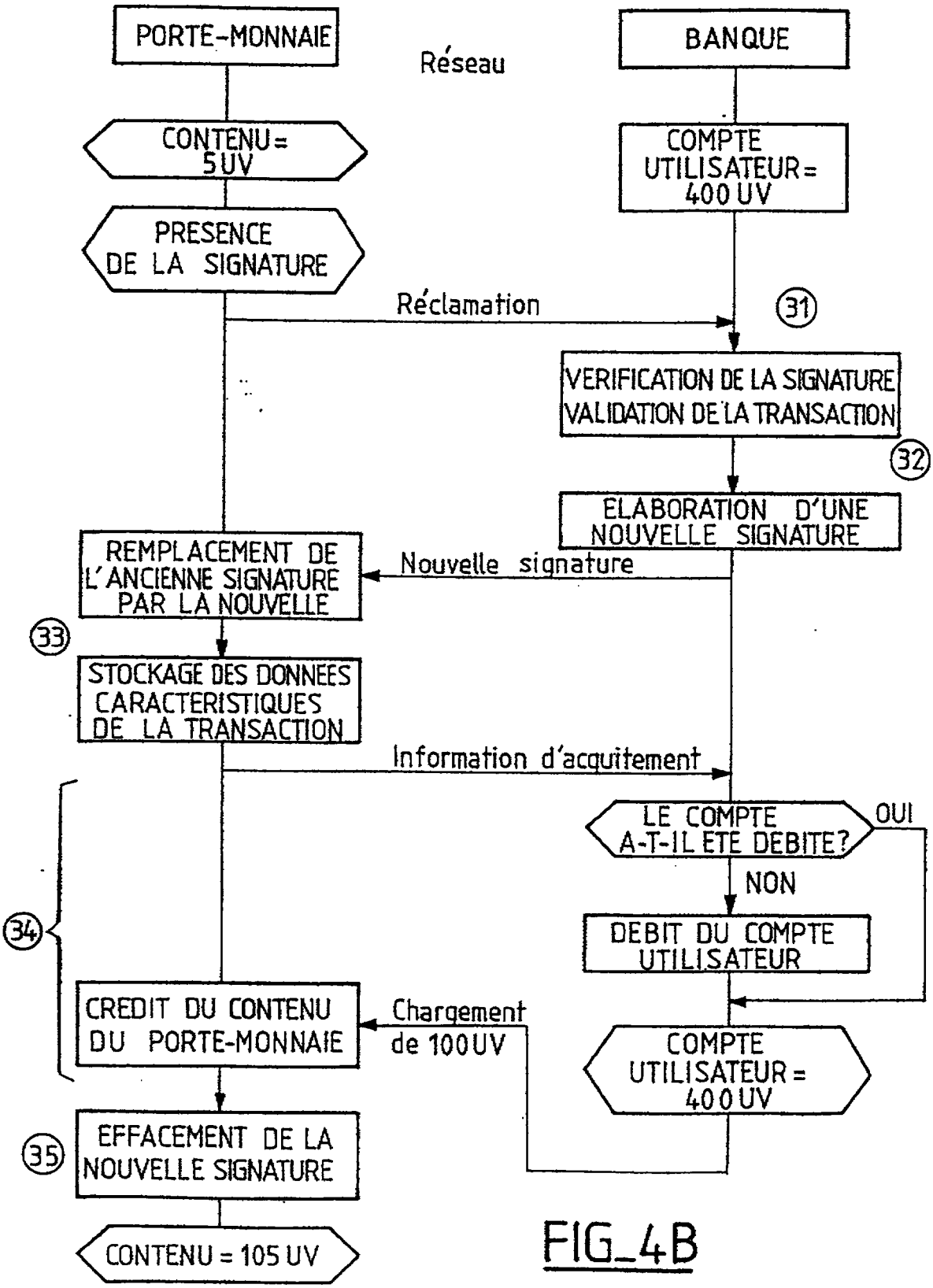
PORTE-MONNAIE
Réseau
BANQUE
CONTENU = 5 UV
COMPTE UTILISATEUR = 400 UV
PRESENCE DE LA SIGNATURE
Réclamation
31
VERIFICATION DE LA SIGNATURE VALIDATION DE LA TRANSACTION
32
ELABORATION D'UNE NOUVELLE SIGNATURE
REMPLACEMENT DE L'ANCIENNE SIGNATURE PAR LA NOUVELLE
Nouvelle signature
33
STOCKAGE DES DONNEES CARACTERISTIQUES DE LA TRANSACTION
Information d'acquitement
LE COMPTE A-T-IL ETE DEBITE?
OUI
NON
34
DEBIT DU COMPTE UTILISATEUR
CREDIT DU CONTENU DU PORTE-MONNAIE
Chargement de 100 UV
COMPTE UTILISATEUR = 400 UV
35
EFFACEMENT DE LA NOUVELLE SIGNATURE
CONTENU = 105 UV

FIG_4B

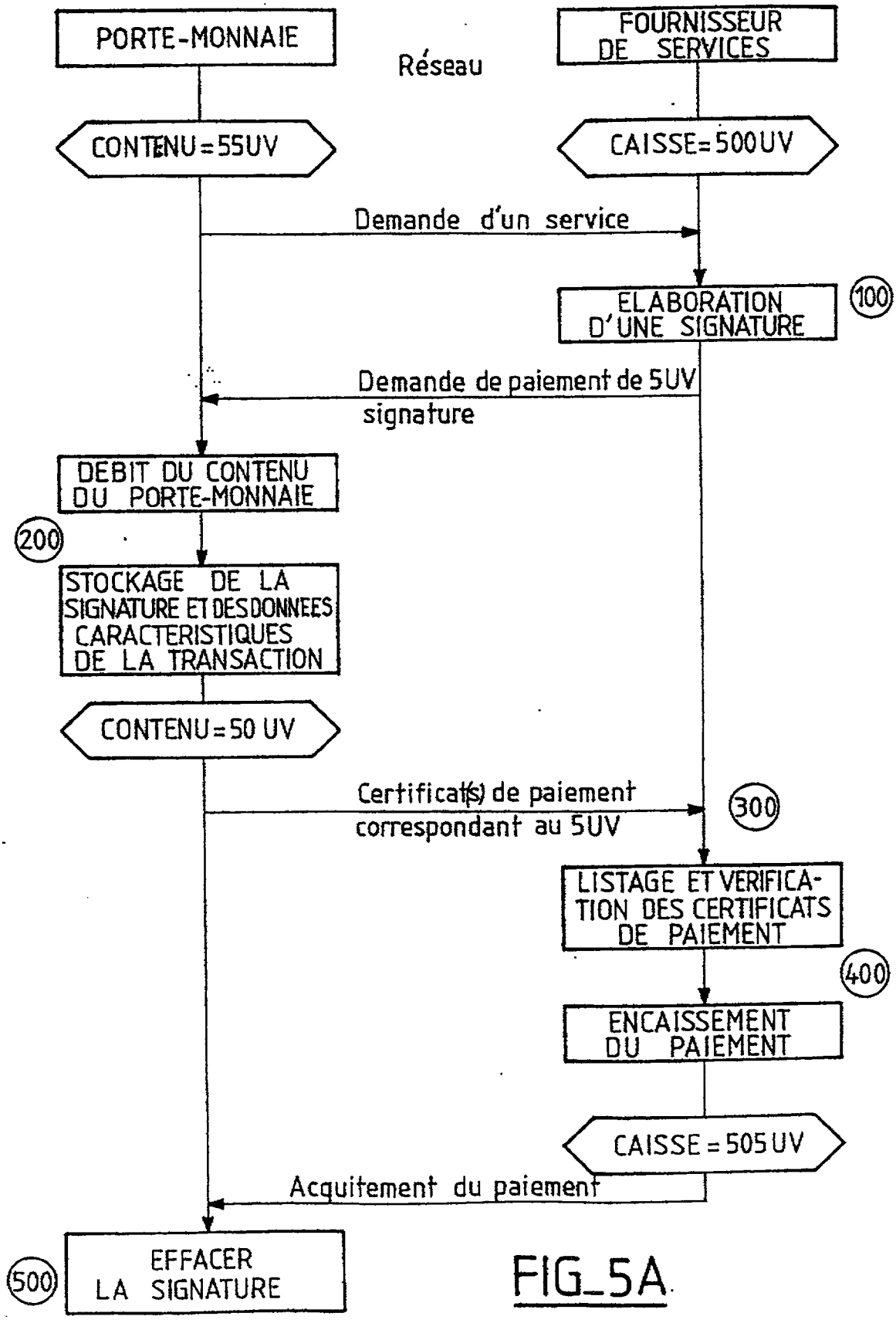
PORTE-MONNAIE
Réseau
FOURNISSEUR DE SERVICES
CONTENU=55UV
CAISSE=500UV
Demande d'un service
ELABORATION D'UNE SIGNATURE
100
Demande de paiement de 5UV signature
DEBIT DU CONTENU DU PORTE-MONNAIE
200
STOCKAGE DE LA SIGNATURE ET DES DONNEES CARACTERISTIQUES DE LA TRANSACTION
CONTENU=50 UV
Certificat(s) de paiement correspondant au 5UV
300
LISTAGE ET VERIFICATION DES CERTIFICATS DE PAIEMENT
400
ENCAISSEMENT DU PAIEMENT
CAISSE=505UV
Acquitement du paiement
500
EFFACER LA SIGNATURE

FIG_5A

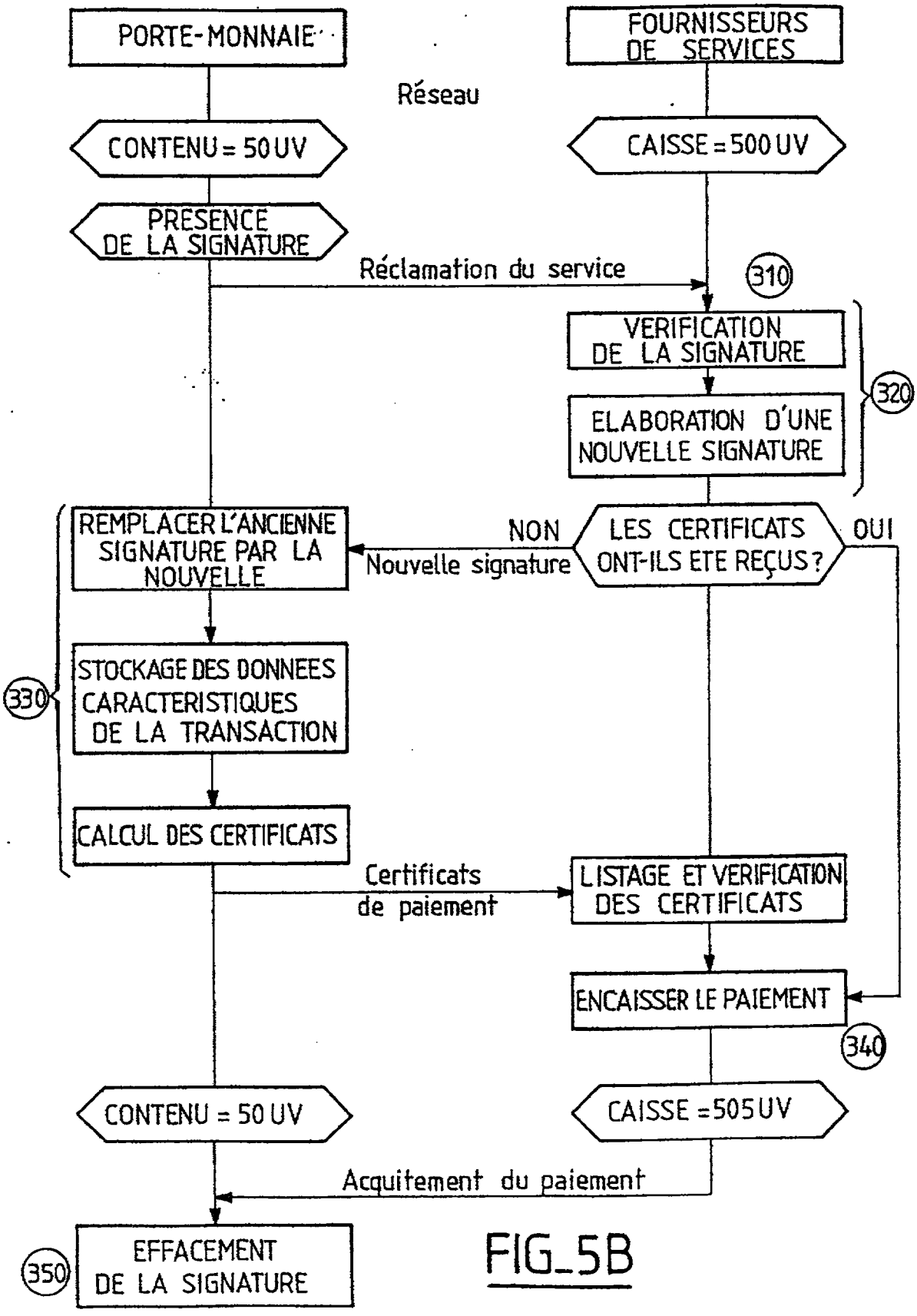
PORTE-MONNAIE
FOURNISSEURS DE SERVICES
Réseau
CONTENU = 50 UV
CAISSE = 500 UV
PRESENCE DE LA SIGNATURE
Réclamation du service
310
VERIFICATION DE LA SIGNATURE
320
ELABORATION D'UNE NOUVELLE SIGNATURE
REMPLACER L'ANCIENNE SIGNATURE PAR LA NOUVELLE
NON
Nouvelle signature
LES CERTIFICATS ONT-ILS ETE REÇUS?
OUI
330
STOCKAGE DES DONNEES CARACTERISTIQUES DE LA TRANSACTION
CALCUL DES CERTIFICATS
Certificats de paiement
LISTAGE ET VERIFICATION DES CERTIFICATS
ENCAISSER LE PAIEMENT
340
CONTENU = 50 UV
CAISSE = 505 UV
Acquitement du paiement
350
EFFACEMENT DE LA SIGNATURE

FIG_5B

METHOD FOR SECURE TRANSFER OF DATA BY A COMMUNICATION NETWORK

The invention concerns data transfers carried out by a communication network. This network may for example be the switched telephone network, a cellular communication network such as the network to the G.S.M. European standard or the INTERNET network.

In cases of conventional exchanges of data between two entities, the authenticity of these exchanged data is guaranteed by an electronic signature. This electronic signature may be obtained using various cryptographic mechanisms such as ciphering or authentification mechanisms or mechanisms involving signatures in the proper sense. The corresponding calculation algorithm may be symmetric, in which case the secret signature key is shared by the two entities, or asymmetric, in which case the secret signature key is known only by the signing entity. Such data transfer methods, allowing the authentification of exchanged data, are notably described in patent application EP-A-0 683 582 and in patent application US 5.534.683.

Today, we are witnessing a great development of mass-market applications on communication networks capable of allowing the use of chip cards. However, the operation of transferring data by a network is difficult to implement since it may consist of

exchanges between a number of entities and a chip card. Moreover, data exchanges by means of a network may be interrupted for many reasons such as, for example, a break in a communication, pulling out of the chip card or a failure of the entity exchanging data with the chip card. This interruption brings about a desynchronization of the two entities to the detriment of one of them. The mechanisms known to date do not allow this desynchronization problem to be avoided in the event of interruption during a data transfer.

The present invention makes it possible to solve this problem of desynchronization of two entities liable to occur at the time of an interruption and proposes a method for secure transfer of data by a communication network, between a first entity constituted by a chip card and a second entity, capable of guaranteeing the use of the chip card under all circumstances even in the event of interruptions during transactions. This method consists of first producing an electronic signature, making it possible to prove the initiation of the transfer, and of storing it in at least one memory area of the chip card and then, when the transfer is complete, of erasing this signature.

According to another characteristic of the invention, the method includes a claim procedure, this procedure consisting of checking the presence or absence of the signature in a memory area of the chip

card, in order to know whether the data transfer has failed or succeeded.

According to another characteristic of the invention, when the data transfer has been interrupted, the claim procedure furthermore consists of:

- producing a new electronic signature,
- replacing the signature of the failed transfer by the said new signature,
- performing the steps of the transfer not yet executed, and then
- erasing the new signature when the transfer is complete.

According to another characteristic of the invention, the signature is stored securely in a memory area so that it is not accessible to the outside world either for reading nor writing.

Advantageously, this memory area is an area of electrically programmable memory of EEPROM type.

According to another characteristic of the invention, the signature is produced by the second entity and erased by the chip card electronics.

According to another characteristic of the invention, the signature may be produced by means of a cryptographic algorithm.

According to another characteristic of the invention, the transferred data are value units. In this case, the chip card may be an electronic purse.

According to another characteristic of the invention, the data transfer method may be applied to a financial transaction between a banking institution and an electronic purse in order to credit the content of the purse, or between a service provider and an electronic purse in order to debit the content of the purse.

According to another characteristic of the invention, the data transfer method may be applied to a transaction of value units between a gaming organisation and a chip card.

The present invention makes it possible to avoid possible unbalances, capable of being created between two entities, caused by interruptions during data transfers. This is because the presence of the electronic signature in a memory area of the chip card, after a transfer operation, indicates the existence of a unbalance and constitutes proof that the operation has failed. Restoration of balance in the exchanges is carried out at the initiative of the user of the chip card. Moreover, an electronic signature corresponding to a transfer can be used only once.

Other particularities and advantages of the invention will emerge from a reading of the description given by way of a non-limitative example with reference to the accompanying figures which depict:

- Figure 1, a schematic diagram of a device for implementing a method according to the invention,

- Figure 2, a flow diagram of a data transfer method according to the invention,

- Figure 3, a flow diagram of a claim procedure making it possible to execute the steps of the transfer method which were interrupted,

- Figure 4A, a flow diagram of a transfer method applied to a financial transaction, between a banking institution and an electronic purse,

- Figure 4B, a flow diagram of a claim procedure allowing the execution of steps which were interrupted during the transaction of Figure 4A,

- Figure 5A, a flow diagram of a transfer method applied to a financial transaction between an electronic purse and a service provider,

- Figure 5B, a flow diagram of a claim procedure allowing the execution of steps which were interrupted during the transaction of Figure 5A.

The data transfer method according to the invention is carried out between two entities, one of which is preferably a chip card.

The chip card used comprises in a known manner a microprocessor connected by a bus to the different memories and to the input/output ports of the card. Among the memories, there is generally:

- a volatile RAM working memory, as in all microprocessor-based systems, for storing the intermediate data necessary during use of the card,

- a ROM read-only memory, containing system programs allowing operation of the card, programs which do not vary from one use to another of the card,

- an EEPROM electrically programmable and erasable memory, for recording data intended to be modified and updated during successive uses of the card.

Figure 1 illustrates a schematic diagram of a device for implementing a data transfer method according to the invention. A chip card C is inserted into the slot of a read/record device referred to subsequently as reader L, which may for example be a computer. The reader L is connected, by means of a network R, to a number of entities E1, E2, ... EN capable of exchanging data with the chip card C.

The flow diagram of Figure 2 illustrates the different steps of a data transfer method according to the invention, between a first entity such as a chip card and a second entity E, by means of a network. In a first step 1, the entity E produces an electronic signature to indicate the initiation of the transfer. The entity then orders the writing of this signature into at least one memory area of the chip card, at step 2. This electronic signature is recorded securely in this memory area, that is to say it is stored so that it is not accessible either for reading nor writing by the outside world. Preferably the memory area in which it is stored is an area of electrically programmable memory of EEPROM type.

The entity E may also have cryptographic algorithms so as to ensure the confidentiality of the signature.

The following steps 3, 4 and 5 consist of performing the data transfer. For this, the entity orders the writing, into another area of the chip card EEPROM memory, of characteristic data of the transfer (step 3). The chip card then sends back acknowledgement information according to which it authorizes the transfer (step 4), and then the transfer is executed (step 5). When the data transfer is complete, the chip card microprocessor orders the erasing of the signature stored in memory (step 5).

If an interruption of the transfer, due to a break in communication, premature pulling out of the chip card or a failure of the entity E for example, occurs between steps 4 and 5, a unbalance might well be created to the detriment of one of the two entities. By virtue of the method according to the invention, such a unbalance can be revealed by the presence of the signature which will not have been erased from the chip card memory. The presence of this signature therefore indicates a possible error situation. Restoration of balance is then performed at the initiative of the user of the card by making a new connection between the two entities by means of the network.

The chip card then orders the execution of a claim procedure, the flow diagram of which is depicted in Figure 3.

First, at step 4a, the entity E checks the presence or absence of the signature in the chip card memory area reserved for it, so as to check whether the data transfer has failed or succeeded.

When the signature is present, that is to say when the transfer has failed, the entity E then produces a new electronic signature and orders the replacement of the first signature corresponding to the failed transfer by this new signature, at step 4b.

The method used, in order to update this signature securely, may for example be the one described in patent application FR 95 01791.

The following step 4c consists of executing the data transfer steps which were interrupted. Finally, when the data transfer has been completely and correctly executed, the new signature is erased (step 4d).

The transferred data may notably be value units.

Advantageously, the chip card may be implemented in electronic purse form.

A particular application of the method according to the invention concerns a financial transaction between an electronic purse (card C) and a banking institution (entity E1) or between an electronic purse and a service providing organisation (entity E2).

In this case, a value unit corresponds, advantageously, to a monetary unit.

A transaction between a purse and a banking institution consists more particularly of crediting the content of the purse, whereas a transaction between this purse and a service providing organisation consists of debiting it.

Management of the storing and erasing of the signature in the EEPROM memory of the electronic purse depends on the type of operation performed. This is because it is different depending on whether the operation consists of crediting or debiting the content of the electronic purse. This management is explained in more detail below.

The flow diagram of Figure 4A illustrates the loading of an electronic purse during a financial transaction with a banking institution.

In the example depicted in this figure, prior to initiation of the transaction, the content of the purse consists of 5 value units VU, and the bank account of the user of the purse consists of 500 VU.

When a user requests the loading of his purse with a value of 100 value units VU for example (step 10), the bank, after having checked the balance of the user account, produces a proof of the transaction, that is to say it calculates an electronic signature, and transmits it to the purse (step 20).

The purse stores the electronic signature and the characteristic data of the transaction in an area of EEPROM memory and sends back to the bank acknowledgement information authorizing execution of the transaction (step 30).

The bank then debits the user account and orders the corresponding loading of the purse (step 40). The crediting is carried out and, simultaneously, the purse erases the signature using the method for secure updating of EEPROM memory described in patent application FR 95 01791.

When the transaction operation is complete, the content of the electronic purse must consequently be equal to 105 VU, while the content of the bank account of the user of the purse is equal to 400 VU.

An interruption between steps 30 and 40 may bring about a unbalance between the purse and the bank to the detriment of the user. This is because it is possible that the bank account of the user has been debited while his purse has not been credited.

However, when such an interruption occurs, since the loading of the purse did not succeed, the signature is not erased from the purse EEPROM memory. The presence of this signature therefore makes it possible to prove that the transaction has failed. The user must then reconnect his purse to the banking institution, by means of the network, in order to restore balance.

At the time of reconnection, the electronic purse microprocessor starts the execution of a claim procedure, the flow diagram of which is illustrated in Figure 4B.

In the example of Figure 4B, the bank account of the user has been debited by 100 VU and is equal to 400 VU, while the content of the purse has not been credited and is still equal to 5 VU.

At the time of the claim, the purse therefore presents to the bank the characteristic data of the transaction and the proof that this transaction was interrupted, that is to say the electronic signature (step 31). The bank checks this electronic signature and validates the claim procedure. Then it produces a new proof of the transaction and transmits it to the purse (step 32).

The purse then stores the new electronic signature, replacing the one corresponding to the failed credit operation, and the characteristic data of the new transaction, and then sends to the bank acknowledgement information authorizing the transaction (step 33). Replacement of the first electronic signature corresponding to the interrupted transaction by the new electronic signature is carried out by means of the method for secure updating of EEPROM memory described in patent application FR 95 01791.

If the bank account of the user was not debited at the time of the first transaction, the bank performs

the debit and then, in all cases, orders the loading of the purse, at step 34.

In the example of Figure 4B, the bank account was debited before interruption of the first transaction. In this case, the bank orders the loading of the content of the purse just after having received the acknowledgement information authorizing the transaction.

The purse erases the new signature of the transaction simultaneously with the credit operation (step 35).

In the same way, a financial transaction may take place between an electronic purse and a service provider. In this case, the service provider, in exchange for a service to be rendered, orders the debiting by a certain value of the content of the purse. This transaction between purse and service provider is depicted in Figure 5A.

When a user requests a service (step 100), the service provider produces a proof of the order, that is to say an electronic signature corresponding to the transaction to be performed.

The purse is next debited by the value corresponding to the service, 5 VU in the example of Figure 5A, and the signature and characteristic data of the transaction are simultaneously recorded in the EEPROM memory of the purse, at step 200.

The purse then issues debit certificates and transmits them to the provider (step 300). The provider checks these certificates, records them and acknowledges the payment (step 400). The payment having been acknowledged, the electronic signature corresponding to the order is erased from the EEPROM memory of the electronic purse (step 500).

If there is a break between steps 300 and 400, the presence of the signature in the EEPROM memory of the purse indicates a possible error situation. This error situation may for example result from the fact that the payment has not been collected by the provider whereas the content of the purse has been debited. However, as long as the provider is not paid, he does not provide the corresponding required service. In order to obtain the service for which he has paid, the user must consequently present the proof of the order, that is to say the electronic signature corresponding to the requested transaction, and possibly re-send the payment certificates if they have not been received by the provider.

The flow diagram of Figure 5B describes the execution of the claim procedure making it possible to complete the payment of a service provider.

In the example in this Figure 5B, the content of the purse has been debited by 5 VU, at the time of the first transaction corresponding to Figure 5A, whereas the payment has not been collected by the provider, the

content of the cash register still being equal to 500 VU. The purse first transmits to the provider the claim information, that is to say the characteristic data of the failed transaction and the signature.

Where the certificate or certificates has or have been received by the provider, the latter acknowledges the payment and the proof of the transaction is erased (steps 340-350).

On the other hand, where the certificate or certificates has or have not been received by the provider, the latter checks the validity of the claim, that is to say the presence of the electronic signature. Furthermore he produces a new electronic signature which he transmits to the purse accompanied by a request for payment, that is to say a request for the certificate or certificates (step 320).

The purse records the characteristic data of the transaction in the EEPROM memory as well as the new electronic signature, replacing the previous one, and recalculates the certificates for the failed debit (step 330).

With the certificates received, recorded and checked, the provider acknowledges the payment (step 340). Finally, the purse erases the proof of the transaction (step 350).

With the claim procedure complete, the content of the purse is debited, the provider has collected the

payment and may therefore render the corresponding service required by the user of the electronic purse.

The examples which have just been described make it possible to understand how management of the storing and erasing of the signature is different depending on the type of operation performed.

Thus, in the case of a credit, erasing of the signature and crediting of the content of the purse are carried out simultaneously.

On the other hand, in the case of a debit, it is recording of the signature and debiting of the content of the purse which are carried out simultaneously.

According to an alternative embodiment, the data transfer method according to the invention may also be applied to a transaction of value units between a gaming organisation and a chip card by means of a network.

In this case, the data transferred are value units each corresponding to a sum of money defined beforehand. Reloading of the content of the chip card is carried out by means of a bank internal to the gaming organisation. Furthermore, the content of the chip card is credited or debited depending on whether the user has won or lost a game. The transactions performed are therefore similar to the financial transactions which have just been described.

An electronic signature, intended to prove that a transaction has failed, can be used only once: the

signature of a failed transaction is replaced by a new electronic claim transaction signature and, in all cases, the signature is erased when the transaction has succeeded.

CLAIMS

1. Method for secure transfer of data by a communication network, between a first entity constituted by a chip card and a second entity,

consisting of first producing an electronic signature, the latter making it possible to prove the initiation of the transfer, and of storing it in at least one memory area of the chip card and then, when the data transfer is complete, of erasing this signature, said method including a claim procedure, this procedure consisting of checking the presence or absence of the electronic signature in a memory area of the chip card, in order to know whether the data transfer has failed or succeeded, characterised in that, when the data transfer has been interrupted, the claim procedure furthermore consists of:

- producing a new electronic signature,
- replacing the signature of the failed transfer by said new signature,
- performing the steps of the transfer not yet executed, and then
- erasing the new signature when the transfer is complete.

2. Method according to Claim 1, characterised in that the signature is stored securely in a memory area so that it is not accessible to the outside world either for reading nor writing.

3. Method according to either of Claims 1 or 2, characterised in that the memory area of the chip card in which the signature is stored is an area of electrically programmable memory of EEPROM type.

4. Method according to one of Claims 1 to 3, characterised in that the electronic signature is produced by a second entity and erased by the chip electronics.

5. Method according to one of Claims 1 to 4, characterised in that the electronic signature is produced by means of a cryptographic algorithm.

6. Method according to one of Claims 1 to 5, characterised in that the transferred data are value units.

7. Method according to one of Claims 1 to 6, characterised in that the chip card is an electronic purse.

8. Application of the method according to one of Claims 1 to 7 to a financial transaction between a banking institution and an electronic purse in order to credit the content of the latter, or between a service provider and an electronic purse in order to debit the content of the latter.

9. Application according to Claim 8, characterised in that where the content of the purse is credited, the credit operation and erasing of the signature are carried out simultaneously.

* C L M S *

10. Application according to Claim 8, characterised in that where the content of the purse is debited, the storage of the signature in a memory area and the debit operation are carried out simultaneously.

11. Application of the method according to one of Claims 1 to 7 to a value unit transaction between a gaming organisation and a chip card.

ABSTRACT

The invention concerns data transfer carried out by a communication network. It concerns in particular a method for safe data transfer by a communication network, between a first entity consisting of a chip card and a second entity, which consists in the preliminary production of an electronic signature for proving the initialisation of the transfer, this signature being stored in at least a memory zone of the chip card, then, when the data transfer is completed, in erasing this signature. The invention is applicable to electronic purses.

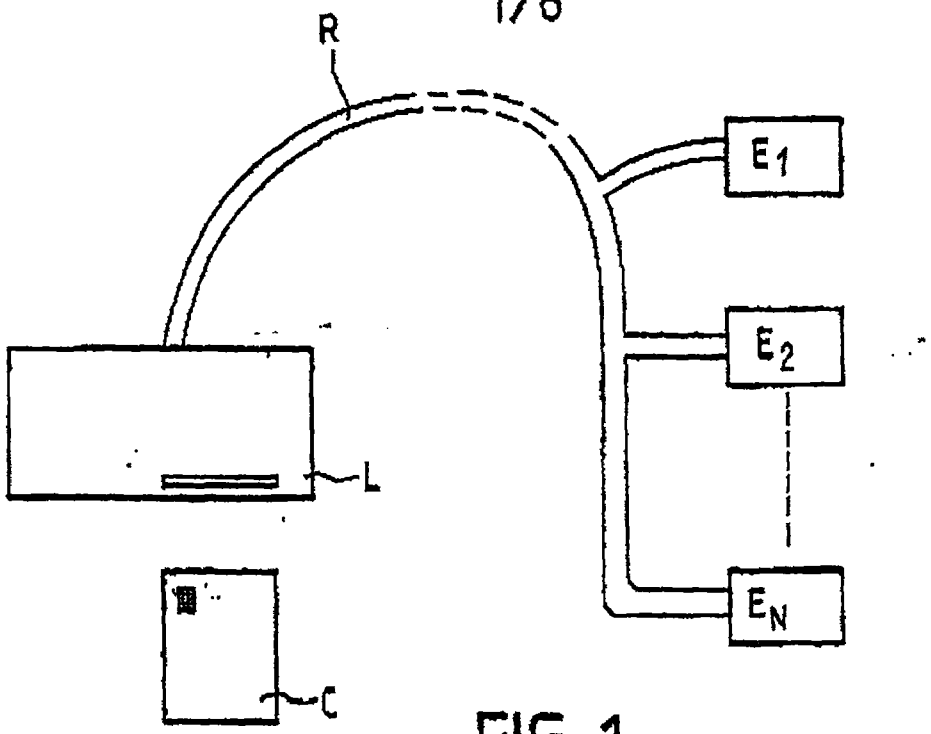
R
E1
E2
EN
L
C

FIG_1

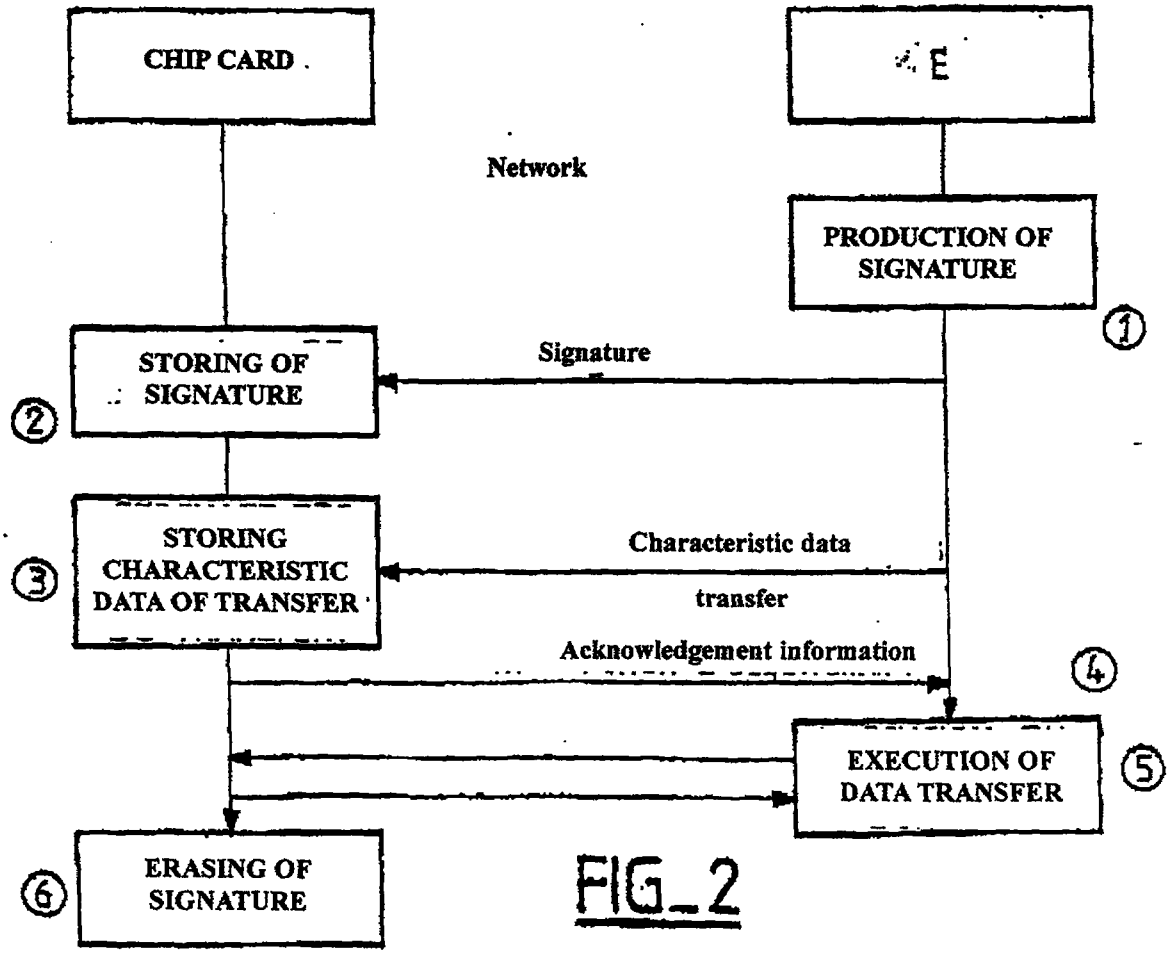
CHIP CARD
E
Network
PRODUCTION OF SIGNATURE
1
Signature
STORING OF SIGNATURE
2
STORING CHARACTERISTIC DATA OF TRANSFER
3
Characteristic data
transfer
Acknowledgement information
4
EXECUTION OF DATA TRANSFER
5
ERASING OF SIGNATURE
6

FIG_2

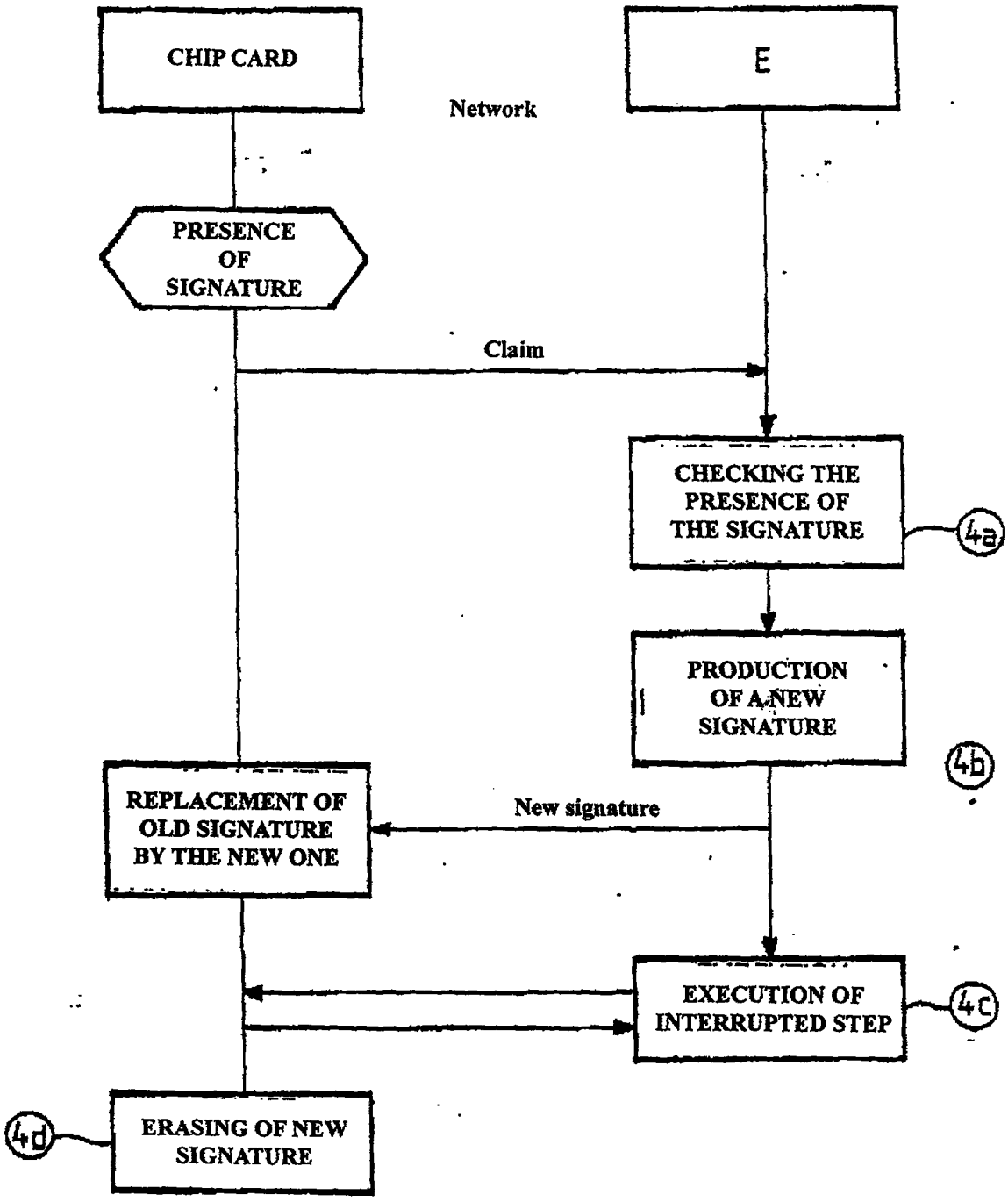
CHIP CARD
Network
E
PRESENCE OF SIGNATURE
Claim
CHECKING THE PRESENCE OF THE SIGNATURE
4a
PRODUCTION OF A NEW SIGNATURE
4b
REPLACEMENT OF OLD SIGNATURE BY THE NEW ONE
New signature
EXECUTION OF INTERRUPTED STEP
4c
4d
ERASING OF NEW SIGNATURE

FIG_3

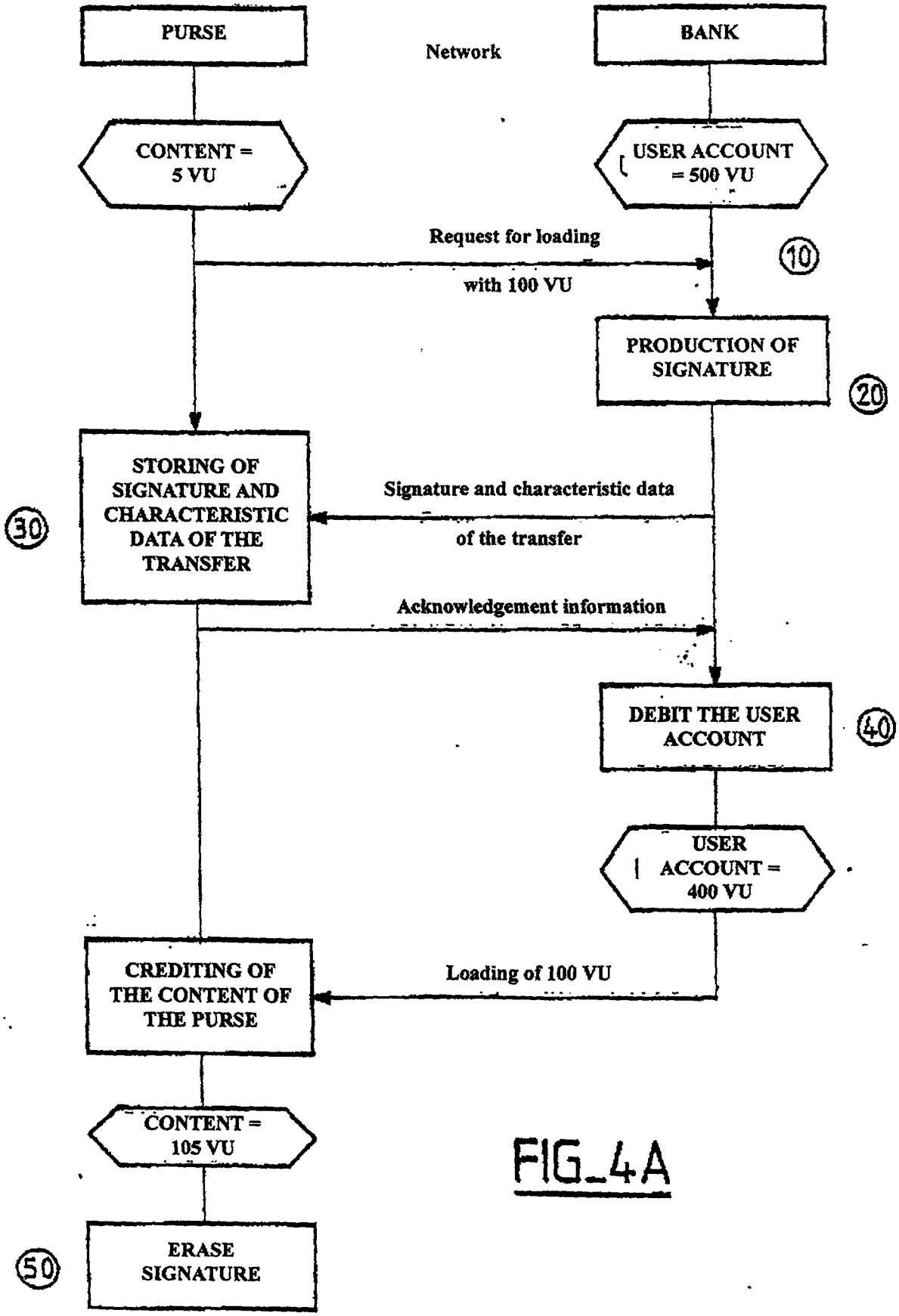
PURSE
Network
BANK
CONTENT = 5 VU
USER ACCOUNT = 500 VU
Request for loading with 100 VU
10
PRODUCTION OF SIGNATURE
20
STORING OF SIGNATURE AND CHARACTERISTIC DATA OF THE TRANSFER
30
Signature and characteristic data of the transfer
Acknowledgement information
DEBIT THE USER ACCOUNT
40
USER ACCOUNT = 400 VU
CREDITING OF THE CONTENT OF THE PURSE
Loading of 100 VU
CONTENT = 105 VU
ERASE SIGNATURE
50

FIG_4A

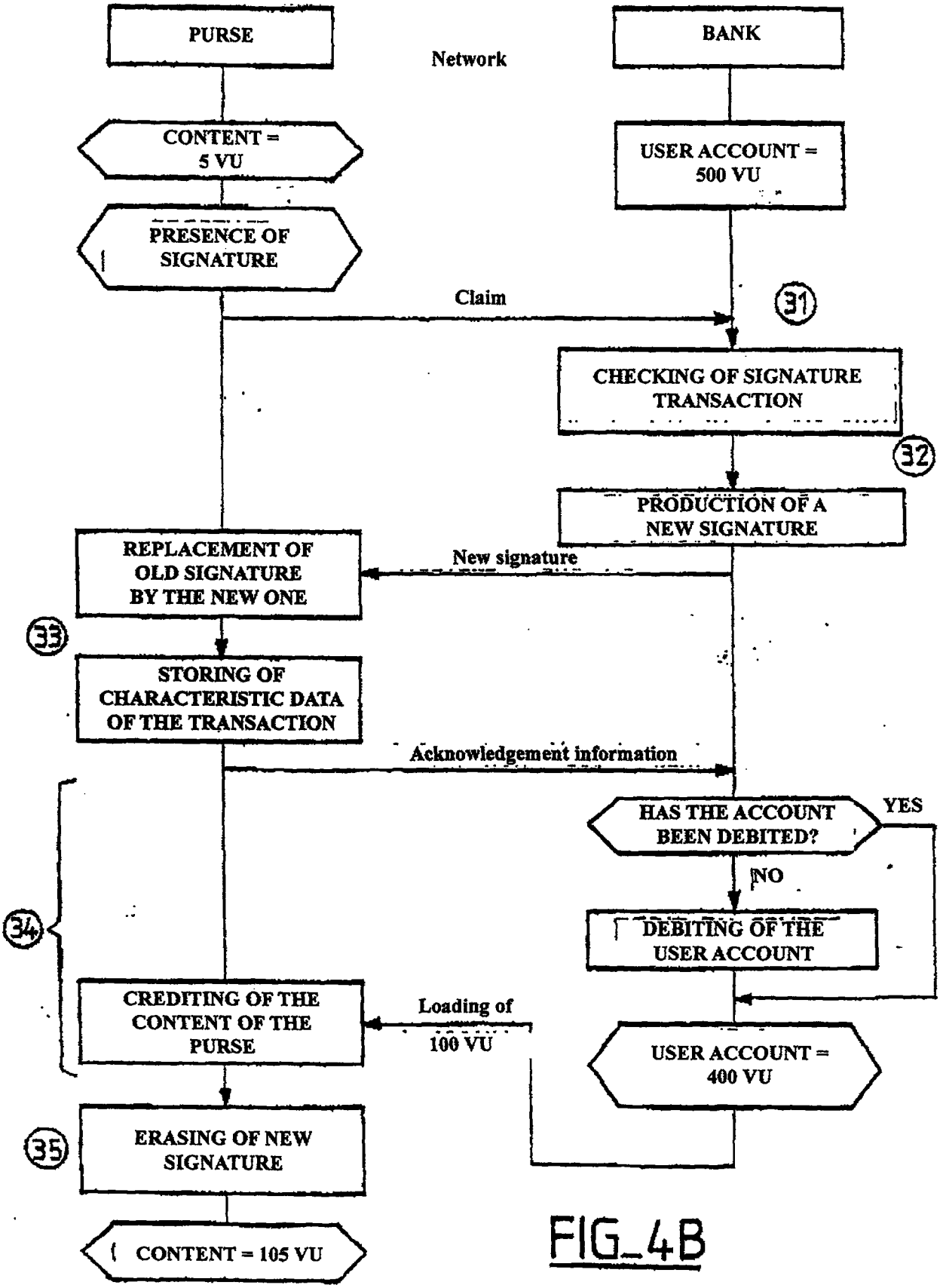
PURSE
Network
BANK
CONTENT = 5 VU
USER ACCOUNT = 500 VU
PRESENCE OF SIGNATURE
Claim
31
CHECKING OF SIGNATURE TRANSACTION
32
PRODUCTION OF A NEW SIGNATURE
New signature
REPLACEMENT OF OLD SIGNATURE BY THE NEW ONE
33
STORING OF CHARACTERISTIC DATA OF THE TRANSACTION
Acknowledgement information
HAS THE ACCOUNT BEEN DEBITED?
YES
NO
34
DEBITING OF THE USER ACCOUNT
CREDITING OF THE CONTENT OF THE PURSE
Loading of 100 VU
USER ACCOUNT = 400 VU
35
ERASING OF NEW SIGNATURE
CONTENT = 105 VU

FIG_4B

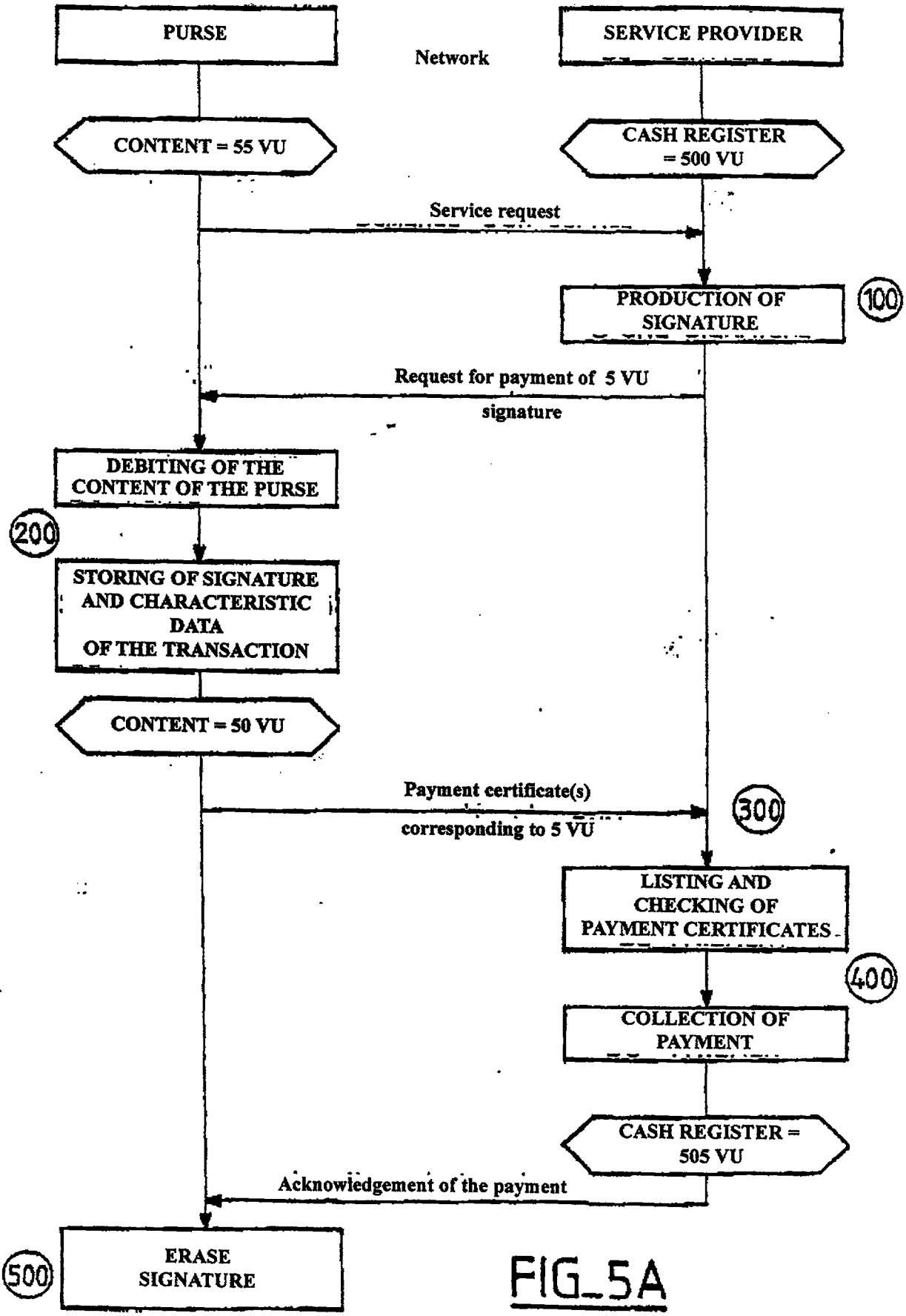
PURSE
Network
SERVICE PROVIDER
CONTENT = 55 VU
CASH REGISTER = 500 VU
Service request
PRODUCTION OF SIGNATURE
100
Request for payment of 5 VU signature
DEBITING OF THE CONTENT OF THE PURSE
200
STORING OF SIGNATURE AND CHARACTERISTIC DATA OF THE TRANSACTION
CONTENT = 50 VU
Payment certificate(s) corresponding to 5 VU
300
LISTING AND CHECKING OF PAYMENT CERTIFICATES
400
COLLECTION OF PAYMENT
CASH REGISTER = 505 VU
Acknowledgement of the payment
500
ERASE SIGNATURE

FIG_5A

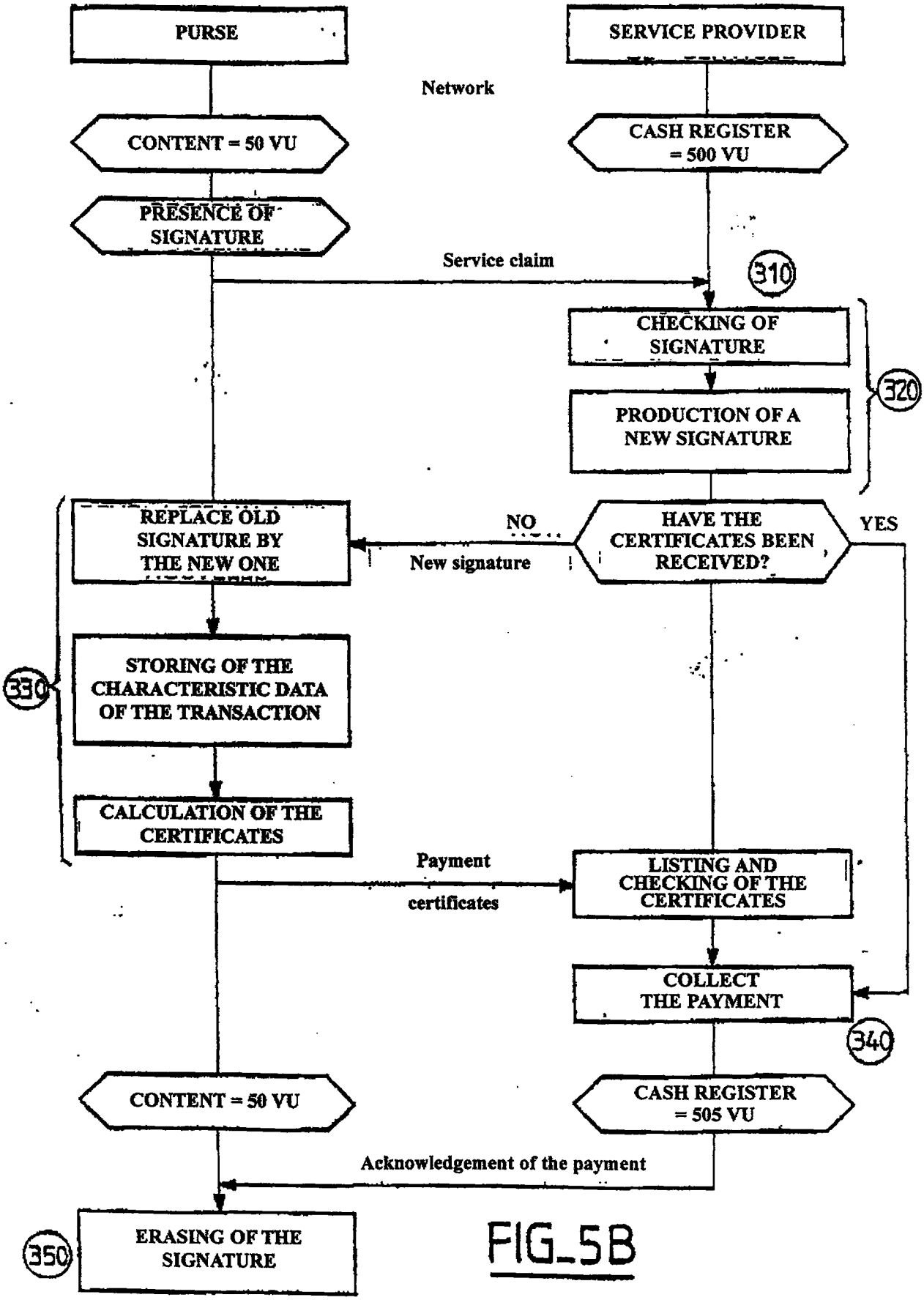
PURSE
SERVICE PROVIDER
Network
CONTENT = 50 VU
CASH REGISTER = 500 VU
PRESENCE OF SIGNATURE
Service claim
310
CHECKING OF SIGNATURE
PRODUCTION OF A NEW SIGNATURE
320
REPLACE OLD SIGNATURE BY THE NEW ONE
NO
HAVE THE CERTIFICATES BEEN RECEIVED?
YES
New signature
330
STORING OF THE CHARACTERISTIC DATA OF THE TRANSACTION
CALCULATION OF THE CERTIFICATES
Payment
certificates
LISTING AND CHECKING OF THE CERTIFICATES
COLLECT THE PAYMENT
340
CONTENT = 50 VU
CASH REGISTER = 505 VU
Acknowledgement of the payment
350
ERASING OF THE SIGNATURE

FIG_5B

980 4 716-0
IPOS 3
copy.

PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 6 : G07F 7/08	A1	(11) Numéro de publication internationale: WO 98/28719 (43) Date de publication internationale: 2 juillet 1998 (02.07.98)

(21) Numéro de la demande internationale: PCT/FR97/02414

(22) Date de dépôt international: 23 décembre 1997 (23.12.97)

(30) Données relatives à la priorité:
96/15980 24 décembre 1996 (24.12.96) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: GEMPLUS S.C.A. [FR/FR]; Parc d'activités de Gémenos, Avenue du Pic de Bertagne, F-13881 Gémenos Cedex (FR).

(72) Inventeur; et
(75) Inventeur/Déposant *(US seulement)*: VANNEL, Pierre [FR/FR]; Charbillac, F-05500 Saint Bonnet (FR).

(74) Mandataire: NONNENMACHER, Bernard; Gemplus S.C.A., Z.I. Athélia III, Voie Antiope, F-13705 La Ciotat Cedex (FR).

(81) Etats désignés: JP, SG, US, brevet européen (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée
Avec rapport de recherche internationale.
Avant l'expiration du délai prévu pour la modification des revendications, sera republiée si de telles modifications sont reçues.

(54) Title: METHOD FOR SECURE TRANSFER OF DATA BY A COMMUNICATION NETWORK

(54) Titre: PROCEDE DE TRANSFERT SECURISE DE DONNEES PAR UN RESEAU DE COMMUNICATION

(57) Abstract

The invention concerns data transfer carried out by a communication network. It concerns in particular a method for safe data transfer by a communication network, between a first entity consisting of a chip card and a second entity, which consists in the preliminary production of an electronic signature for proving the initialisation of the transfer, this signature being stored in a least a memory zone of the chip card, then, when the data transfer is completed, in erasing this signature. The invention is applicable to electronic purse.

(57) Abrégé

L'invention concerne les transferts de données réalisés par un réseau de communications. Elle concerne notamment un procédé de transfert sécurisé de données par un réseau de communications, entre une première entité constituée par une carte à puce et une deuxième entité, selon lequel on élabore au préalable une signature électronique, permettant de prouver l'initialisation du transfert, cette signature étant stockée dans au moins une zone mémoire de la carte à puce puis, lorsque le transfert de données est terminé, on efface cette signature. Application au porte-monnaie électronique.

