

12

DEMANDE DE BREVET D'INVENTION

A1

22 Date de dépôt : 07.07.00.

30 Priorité :

43 Date de mise à la disposition du public de la demande : 11.01.02 Bulletin 02/02.

56 Liste des documents cités dans le rapport de recherche préliminaire : *Se reporter à la fin du présent fascicule*

60 Références à d'autres documents nationaux apparentés :

71 Demandeur(s) : THOMSON MULTIMEDIA Société anonyme — FR.

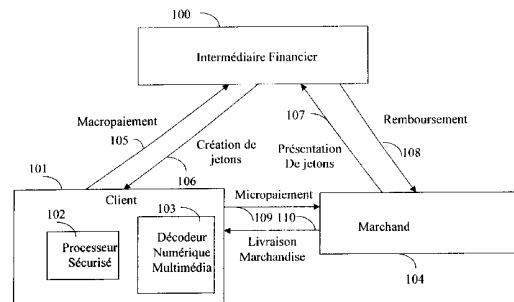
72 Inventeur(s) : VIGOUROUX JEAN RENAN.

73 Titulaire(s) :

74 Mandataire(s) :

54 SYSTEME ET PROCEDE DE GESTION DE TRANSACTION DE MICROPAIEMENT, DISPOSITIFS CLIENT, MARCHAND ET INTERMEDIAIRE FINANCIER.

57 Pour gérer des transactions de micropaiement, entre un marchand (104) et au moins un client (101, 201), on met en oeuvre pour chaque nouvelle transaction un moyen d'allocation de nouveau numéro de transaction (TO) qui suit selon un ordre préétabli de numérotation un dernier numéro mémorisé (LTO) et un moyen de mise à jour du registre de dernier numéro mémorisé (LTO), le moyen de mise à jour enregistrant le nouveau numéro de transaction (TO) étant susceptible d'être vérifié par un intermédiaire financier (100).



La présente invention se rapporte au domaine de la gestion des transactions de micropaiements.

Plus précisément, l'invention concerne plus particulièrement un système, un procédé et des dispositifs de gestion de transaction de micropaiement mettant en œuvre au moins un client susceptible d'effectuer une transaction de micropaiement avec un marchand de biens et/ou de services, cette transaction étant validée par un intermédiaire financier (en anglais « broker ») et s'effectuant sous forme de jetons représentant une unité de paiement.

Selon un deuxième aspect, l'invention concerne un terminal numérique multimédia possédant au moins un processeur sécurisé et adapté en tant que client à effectuer des transactions de micropaiement. Le terminal pouvant être notamment un décodeur numérique multimédia (en anglais « set top box »). Le processeur sécurisé est amovible (par exemple lorsqu'il s'agit d'une carte à puce) ou fixe.

Par micropaiement, on entend ici un paiement d'un montant réduit, par exemple de quelques centimes à quelques dizaines ou centaines de francs (ou d'un montant réduit dans toute autre monnaie d'échange).

L'émergence des systèmes de transactions de micropaiement mis en œuvre par le biais de réseaux de communication, tels que par exemple le réseau mondial Internet, a soulevé le problème de la sécurité des transactions entre clients et marchands, ainsi que de la sécurité des informations échangées au cours de ces transactions. Par ailleurs, la faiblesse des montants de transactions de micropaiement nécessite des solutions relativement légères à mettre en œuvre.

Notamment l'un des problèmes principaux de la sécurité des transactions est la possibilité pour un marchand de copier un jeton et de l'utiliser frauduleusement. De nombreux systèmes de gestion des transactions de micropaiement ont été proposées pour qu'il n'y ait pas duplication des retraits d'argent correspondant à une seule transaction. Ces systèmes sont par exemple décrits dans le livre, "Electronic payment system" écrit par Donal O'Mahony, Michael Peirce et Hitesh Tewari, publié chez Artech House en 1997. Le chapitre 6 de cet ouvrage, « electronic cash payment system » décrit plusieurs méthodes anti-duplication, dans des systèmes de paiement cash, notamment les systèmes Ecash, CAFE et Netcash.

Dans le système Ecash de la société Digicash, le client génère un numéro de série aléatoire qu'il affecte à chaque pièce de monnaie électronique susceptible d'être utilisée tel que la probabilité d'avoir deux fois le même numéro est très faible. Ces pièces sont délivrées par une banque ou un
5 intermédiaire financier. Pour éviter la duplication des pièces électroniques par un client, la banque doit enregistrer le numéro de série de chaque pièce qui est y déposée. Cela nécessite l'utilisation de bases de données énormes.

Sur des systèmes très sécurisés tel que le projet CAFE (En anglais « Conditional Access For Europe ») utilisant entre autres la cryptographie et
10 par exemple des cartes à puces, les intermédiaires financiers conservent une base de données relatives aux derniers paiements effectués. Même si les bases de données du projet CAFE sont plus réduites que dans le système Ecash, leur gestion reste lourde.

Dans le système Netcash, un serveur d'argent conserve en mémoire
15 les numéros de série des pièces de monnaie électroniques qu'il a lui-même mises en circulation et auxquelles il a attribué un numéro de série. Cela nécessite aussi une base de donnée de grande taille.

Dans ce même ouvrage, le chapitre 7, "Micropayment systems", décrit des méthodes anti-duplication plus adaptées aux systèmes de micropaiement,
20 notamment les systèmes Millicent, SubScrip, PayWord et MicroMint.

Dans le schéma Millicent développé par la société Digital Equipment Corporation, le marchand vérifie qu'une unité de monnaie ayant un identificateur donné qui correspond à un numéro de série n'a pas déjà été
25 dépensée. Aussi, le marchand doit maintenir une base de données contenant les identificateurs des unités de monnaie émises.

Dans le système SubScrip développé par l'université de Newcastle en Australie, le marchand possède une base de données contenant tous les identificateurs de monnaie valides.

Dans le système PayWord développé par le MIT aux Etats Unis et
30 l'institut des sciences Weizman en Israël, le micropaiement est basé sur l'utilisation de crédit qui permet la délivrance de certificats Payword. Ces certificats sont ensuite utilisés par un utilisateur pour construire des chaînes Payword qui serviront aux paiements et permettront au marchand de vérifier la validité de ceux-ci. La complexité réside ici dans la gestion des certificats.

35 Dans le système MicroMint développé par le MIT aux Etats Unis et l'institut des sciences Weizman en Israël, c'est l'intermédiaire financier qui

vérifie si deux transactions n'ont pas été dupliquées. Néanmoins, celle-ci est basée sur la non conservation de l'anonymat du client. En cas de fraude, l'intermédiaire financier ne pourra cependant pas distinguer si c'est un client ou un marchand qui en est responsable.

5 Il existe de nombreux systèmes et procédés de gestion de transaction de micropaiement, présentant des niveaux de sécurité et de complexité divers et dans lesquels un client dispose d'un porte-monnaie électronique. Mais, on ne connaît à ce jour aucun système ou protocole de mise en œuvre simple, présentant une sécurité satisfaisante pour les différents acteurs des
10 transactions (intermédiaire financier, client, marchand).

D'une manière générale, un inconvénient des mécanismes anti-duplication de l'art antérieur est la lourdeur de leur mise en œuvre (des bases de données de taille importantes mémorisant des numéros de transactions ou de jetons sont notamment nécessaires) ou la non préservation de l'anonymat
15 des clients.

Par ailleurs, un inconvénient des systèmes à micropaiement est qu'ils nécessitent un terminal dédié à l'interfaçage avec un processeur sécurisé propre au client.

L'invention selon ses différents aspects a notamment pour objectif de
20 pallier ces inconvénients de l'art antérieur.

Plus précisément, un objectif de l'invention est de fournir un système et un procédé de gestion des transactions de micropaiement qui soient simples, faciles d'utilisation et peu coûteux à mettre en œuvre.

L'invention a notamment pour objectif la sécurisation des transactions
25 entre un marchand et un intermédiaire financier qui soit simple à mettre en œuvre et ne nécessite pas l'utilisation de bases de données de taille importante ou de nombreuses opérations à effectuer.

Un autre objectif de l'invention est l'adaptation des moyens de sécurisation à un indice de fiabilité propre à chaque marchand.

30 L'invention a encore pour objectif de sécuriser les transactions coté client tout en préservant son anonymat.

Dans ce but, l'invention propose un procédé de gestion de transaction de micropaiement, entre un marchand et au moins un client remarquable en ce qu'à chaque nouvelle transaction,

35 - le marchand alloue un nouveau numéro de transaction qui suit selon un ordre préétabli de numérotation un dernier numéro mémorisé et

- le marchand met à jour un registre de dernier numéro mémorisé en enregistrant le nouveau numéro de transaction,
- chaque numéro de transaction étant susceptible d'être vérifié par un intermédiaire financier.

5 Ainsi, l'invention permet avantageusement d'allouer d'une manière simple des numéros de transactions qui pourront être facilement vérifiées pour éviter les duplications. Ainsi, tout en ayant une bonne sécurité dans les transactions, ni le marchand, ni l'intermédiaire financier n'ont besoin de gérer de bases de données de grande taille. De plus, l'anonymat du client est
10 conservé vis-à-vis du marchand.

 Selon une caractéristique particulière, le procédé de gestion de transaction de micropaiement est remarquable en ce qu'au moins un client parmi lesdits clients est un terminal multimédia numérique et/ou analogique.

 Ainsi, de façon avantageuse, l'invention se prête bien à tout type de
15 transactions de micropaiement et notamment aux transactions impliquant un client de type terminal multimédia numérique et/ou analogique, par exemple un décodeur multimédia numérique.

 Selon une caractéristique particulière, le procédé de gestion de transaction de micropaiement est remarquable en ce que le terminal
20 multimédia comprend au moins un processeur sécurisé fixe ou amovible nécessaire à la mise en œuvre desdites transactions de micropaiement.

 Ainsi, l'invention se prête avantageusement au cas où le terminal est équipé d'un lecteur de processeur sécurisé ce qui est généralement le cas des décodeurs multimédia numériques et/ou s'il contient lui-même un
25 processeur sécurisé. On a ainsi en outre une grande souplesse d'utilisation de ce terminal pour effectuer des transactions de micropaiements.

 Selon une caractéristique particulière, le procédé de gestion de transaction de micropaiement est remarquable en ce que le marchand est équipé d'un lecteur de processeur sécurisé amovible.

30 Selon une caractéristique particulière, le procédé de gestion de transaction de micropaiement est remarquable en ce qu'au moins un client est un processeur sécurisé amovible lisible par le lecteur de processeur sécurisé amovible du marchand.

 Ainsi, dans ce mode de réalisation avantageux de l'invention, le client
35 peut effectuer la transaction directement chez le marchand tout en ayant une grande sécurité dans les transactions.

Selon une caractéristique particulière, le procédé de gestion de transaction de micropaiement entre un client et un marchand par un intermédiaire financier est remarquable en ce que pour un premier ensemble d'au moins une transaction réalisée par le marchand et possédant un numéro de transaction alloué par le marchand, l'intermédiaire financier effectue pour
5 chaque transaction du premier ensemble

- au cours d'une première étape, une opération de vérification de ladite transaction consistant à déterminer si ledit numéro de transaction suit selon un ordre préétabli un dernier numéro de
10 transaction enregistré puis
- au cours d'une deuxième étape,
 - lorsque le résultat de ladite opération de vérification est négatif, une opération de rejet de ladite transaction
 - et lorsque le résultat de ladite opération de vérification est positif,
15 une opération d'enregistrement dudit numéro de transaction en tant que dernier numéro de transaction pour ledit marchand.

Ainsi, l'intermédiaire financier peut avantageusement vérifier la validité d'une transaction pour la rejeter si elle n'est pas valide et éviter la duplication des transactions.

20 Selon une caractéristique particulière de l'invention, le procédé de gestion de transaction de micropaiement est remarquable en ce que l'opération de vérification de la transaction comprend en outre une opération de vérification de signature de la transaction.

Ainsi, on peut avantageusement, effectuer des vérifications
25 complémentaires pour détecter une éventuelle fraude.

Selon une caractéristique particulière, le procédé de gestion de transaction de micropaiement est remarquable en ce que l'opération de vérification de la transaction est effectuée selon un indice de fiabilité du marchand.

30 Ainsi, l'invention permet avantageusement de limiter le nombre de vérifications quand un marchand est fiable et de se polariser sur les marchands les moins fiables.

Selon une caractéristique particulière, le procédé de gestion de transaction de micropaiement est remarquable en ce que la vérification de
35 signature de la transaction est effectuée :

- systématiquement si l'indice de fiabilité du marchand est inférieur à un seuil ;
- selon un mécanisme non systématique si l'indice de fiabilité du marchand est supérieur au dit seuil.

5 Ainsi, l'intermédiaire financier peut avantageusement effectuer de manière pragmatique les vérifications les plus complexes en fonction de la fiabilité du marchand.

 Selon une caractéristique particulière, le procédé de gestion de transaction de micropaiement est remarquable en ce que lorsque le résultat
10 de l'opération de vérification de signature de la transaction est négatif, le procédé comprend en outre une opération de vérification des signatures d'un deuxième ensemble de transactions.

 Selon une caractéristique particulière, le procédé de gestion de transaction de micropaiement est remarquable en ce que le deuxième
15 ensemble de transactions comprend toutes les transactions présentées par le marchand à l'intermédiaire financier depuis une transaction de référence et dont la signature n'a pas déjà été vérifiée

 Selon une caractéristique particulière, le procédé de gestion de transaction de micropaiement est remarquable en ce que la transaction de
20 référence est :

- la dernière transaction ayant reçu une acceptation de paiement ;
et/ou
- la dernière transaction précédant la transaction de micropaiement dont la signature a été vérifiée.

25 Ainsi, de façon avantageuse, l'intermédiaire financier peut effectuer des vérifications complémentaires et appropriées quand la fiabilité du marchand est remise en cause.

 Selon une caractéristique particulière, le procédé de gestion de transaction de micropaiement est remarquable en ce que l'intermédiaire
30 financier est susceptible de mettre à jour la fiabilité du marchand en fonction du résultat d'au moins une des vérifications de signature.

 Ainsi, préférentiellement, l'indice de fiabilité évolue et la vérification des transactions est adaptative.

35 Selon une caractéristique particulière, le procédé de gestion de transaction de micropaiement est remarquable en ce que l'ordre préétabli a

été établi par le marchand ou l'intermédiaire financier ou un opérateur technique.

Ainsi, de façon avantageuse, l'ordre préétabli peut être défini par l'un des intervenants majeurs dans les transactions ou dans la mise en œuvre de moyens permettant des transactions. On peut de cette manière optimiser l'ordre établi selon un critère propre à l'un des intervenants.

Selon une caractéristique particulière, le procédé de gestion de transaction de micropaiement est remarquable en ce que ledit ordre préétabli est l'ordre naturel des entiers croissants et/ou un ordre chronologique de type heure et/ou date.

Ainsi, on peut avantageusement avoir un ordre préétabli permettant une mise en œuvre simple du procédé de gestion de transaction.

Selon une caractéristique particulière, le procédé de gestion de transaction de micropaiement est remarquable en ce que l'ordre préétabli est un ordre en boucle.

Ainsi, d'une façon avantageuse, on simplifie la taille des numéros de transactions tout en évitant tout risque de dépassement d'une valeur maximale.

L'invention propose en outre un système remarquable en ce qu'il comprend des moyens adaptés à la mise en œuvre du procédé de gestion de transaction de micropaiement décrit précédemment.

L'invention propose en outre un dispositif de gestion de transaction de micropaiement, entre le dispositif et au moins un client remarquable en ce qu'il comprend pour chaque nouvelle transaction,

- un moyen d'allocation de nouveau numéro de transaction qui suit selon un ordre préétabli de numérotation un dernier numéro mémorisé ; et
- un moyen de mise à jour du registre de dernier numéro mémorisé le moyen de mise à jour enregistrant le nouveau numéro de transaction ;

chaque numéro de transaction étant susceptible d'être vérifié par un intermédiaire financier.

L'invention propose en outre un dispositif de gestion de transaction de micropaiement entre un client et un marchand remarquable en ce que pour un premier ensemble de transactions réalisées par le marchand et possédant un

numéro de transaction alloué par le marchand, le dispositif comprend pour chaque transaction du premier ensemble

- 5 - un moyen de vérification de la transaction adapté à déterminer si le numéro de transaction suit selon un ordre préétabli un dernier numéro de transaction enregistré ;
- lorsque le résultat de l'opération de vérification est négatif, un moyen de rejet de la transaction ;
- 10 - et lorsque le résultat de l'opération de vérification est positif, un moyen d'enregistrement du numéro de transaction en tant que dernier numéro de transaction pour le marchand.

Les caractéristiques particulières et les avantages des dispositifs et du système de gestion de transaction de micropaiement étant les mêmes que ceux du procédé de gestion de transaction de micropaiement, ils ne sont pas rappelés ici.

15 L'invention propose en outre un terminal numérique multimédia remarquable en ce qu'il comprend au moins un processeur sécurisé fixe ou amovible et que ledit processeur sécurisé est adapté à effectuer des transactions de micropaiements en tant que client.

20 Selon une caractéristique particulière, le terminal numérique multimédia est remarquable en ce qu'il est un décodeur numérique multimédia.

 Ainsi, de façon avantageuse, un terminal multimédia notamment quand il s'agit d'un décodeur numérique multimédia peut être facilement utilisé pour effectuer des transactions de micropaiement. En outre bien souvent, un tel terminal possède un lecteur de cartes à puces dédiées à des transactions
25 vers un marchand donné. L'adaptation d'un tel terminal pour des transactions de micropaiement selon l'invention est relativement simple et peu coûteuse à mettre en œuvre.

 D'autres caractéristiques et avantages de l'invention apparaîtront plus clairement à la lecture de la description suivante d'un mode de réalisation
30 préférentiel, donné à titre de simple exemple illustratif et non limitatif, et des dessins annexés, parmi lesquels :

 la figure 1 présente un synoptique général d'une transaction de micropaiement entre un client, un marchand et un intermédiaire financier, conforme à l'invention selon un mode particulier de réalisation ;

la figure 2 présente un synoptique général d'une transaction de micropaiement selon une première variante, conforme à l'invention selon un mode particulier de réalisation ;

5 la figure 3 présente un décodeur numérique multimédia avec lecteur de processeur sécurisé amovible (client), conforme à l'invention selon un mode particulier de réalisation ;

la figure 4 présente un décodeur numérique multimédia avec processeur sécurisé intégré (client), conforme à l'invention selon un mode particulier de réalisation ;

10 la figure 5 présente un processeur sécurisé (client), conforme à l'invention selon un mode particulier de réalisation ;

la figure 6 présente un schéma d'un dispositif de type marchand, conforme à l'invention selon un mode particulier de réalisation ;

15 la figure 7 présente un schéma d'un dispositif de type marchand avec lecteur intégré de processeur amovible selon la première variante, conforme à l'invention selon un mode particulier de réalisation ;

la figure 8 présente un schéma d'un dispositif de type intermédiaire financier, conforme à l'invention selon un mode particulier de réalisation ;

20 la figure 9 présente un protocole de chargement des jetons sur un processeur sécurisé, conforme à l'invention selon un mode particulier de réalisation ;

la figure 10 présente un protocole de dépense des jetons sur un processeur sécurisé, conforme à l'invention selon un mode particulier de réalisation ;

25 la figure 11 présente un protocole de rachat des jetons au marchand, conforme à l'invention selon un mode particulier de réalisation ;

la figure 12 présente un organigramme de génération des numéros de transactions par le marchand, conforme à l'invention selon un mode particulier de réalisation ;

30 la figure 13 présente un organigramme de validation de transactions par l'intermédiaire financier, conforme à l'invention selon un mode particulier de réalisation ;

35 la figure 14 présente un organigramme de validation de transactions par l'intermédiaire financier selon une deuxième variante, conforme à l'invention selon un mode particulier de réalisation ;

Le principe général de l'invention selon son premier aspect repose sur l'attribution de numéros de transaction par un marchand selon un ordre préétabli. Le marchand n'a besoin de mémoriser qu'un dernier numéro attribué. Un intermédiaire financier vérifie qu'une transaction n'a pas été
5 dupliquée en testant les numéros de transactions : deux transactions provenant du même marchand ne peuvent avoir le même numéro. Il suffit alors que l'intermédiaire financier garde en mémoire le dernier numéro de transaction en provenance d'un marchand et le compare au numéro d'une
10 nouvelle transaction en provenance du même marchand pour valider cette nouvelle transaction. L'intermédiaire financier peut par ailleurs effectuer des vérifications complémentaires telles que des vérifications de signature. Ces vérifications étant plus lourdes à mettre en œuvre, l'intermédiaire financier peut adapter leur fréquence à un indice de fiabilité de chaque marchand qu'il met à jour lui-même.

15 Selon un deuxième aspect, l'invention met en œuvre un client de type terminal numérique multimédia pouvant être notamment un décodeur numérique multimédia, ce client étant susceptible d'effectuer des transactions de micropaiement. Ce client comprend notamment au moins un processeur sécurisé. Généralement, les décodeurs numériques possèdent un lecteur de
20 carte à puces pour des transactions vers un fournisseur de contenu numérique tel que, par exemple, un programme de télévision. Conformément à l'invention, ce lecteur est utilisé pour des transactions de micropaiement moyennant des adaptations peu coûteuses.

On note que dans le mode préféré de réalisation, un processeur
25 sécurisé fixe ou amovible adapté à effectuer des transactions de micropaiement en tant que client met en œuvre une paire de clés asymétriques qu'il possède en propre (cryptographie asymétrique) et qu'il utilise pour les transactions de micropaiement.

On présente, en relation avec la figure 1 un synoptique général de
30 transaction de micropaiement mettant en œuvre un client 101, un marchand 104 et un intermédiaire financier 100. Par souci de clarté, on assimile les terminaux ou dispositifs et leur fonction ; ainsi, le client 101, le marchand 104 et l'intermédiaire financier 100 sont des terminaux ou dispositifs.

Pour participer à une transaction de micropaiement, le client 101 est un
35 terminal numérique multimédia qui comprend deux entités :

- un processeur sécurisé fixe ou amovible 102 , utilisé comme moyen de stockage de données sécurisées et comme moyen d'authentification du client 101. On peut envisager que ce processeur sécurisé ait d'autres fonctionnalités, telles que par exemple la gestion de l'accès conditionnel à des programmes de télévision ;
- un décodeur numérique multimédia pouvant communiquer avec le marchand 104 et l'intermédiaire financier 100 via un réseau.

Le décodeur numérique multimédia 103 est généralement muni d'un lecteur de type carte à puce pour des transactions de type paiement d'émissions de télévision à la carte (en anglais « pay-per-view »). Dans ce cas, la carte à puce est dédiée aux transactions avec un marchand unique, de type opérateur de télévision. Néanmoins, conformément à l'invention, ce lecteur utilise un processeur sécurisé amovible 102 pour effectuer des transactions de micropaiement avec un marchand de services ou de biens quelconques.

Selon une variante de mise en œuvre, le décodeur numérique multimédia 103 intègre un processeur sécurisé 102 fixe.

On notera que le bloc référencé 100 de la figure 1 représente, par souci de simplification, l'intermédiaire financier ou la banque du client 101 et/ou du marchand 104. On peut bien sûr envisager que le client 101 et le marchand 104 soient clients du même intermédiaire financier ou d'intermédiaires financiers différents. Par la suite, on suppose que le client 101 et le marchand 104 ont le même intermédiaire financier.

Le client possède un porte-monnaie électronique pour effectuer ses transactions de micropaiement. Ce porte-monnaie est géré par le processeur sécurisé 102.

Avant tout achat, si son porte-monnaie est vide ou insuffisamment approvisionné, le client 101 doit se procurer des jetons auprès d'un intermédiaire financier 100. Dans ce dessein, le client 101 effectue une requête de macropaiement 105 à l'intermédiaire financier 100. Cette requête constitue une autorisation à débiter un compte bancaire qui est propre au client 101 d'un montant égal à la valeur des jetons qu'il souhaite acquérir.

Si la requête est valide, l'intermédiaire financier 100, transmet les jetons 106 au client 101 dont le porte-monnaie sera crédité de la somme requise.

Après avoir effectué une requête d'achat auprès du marchand 104, le client 101 effectue une transaction de micropaiement 109 puis si la transaction est valide le marchand délivre la marchandise 110 au client 101.

5 Pour créditer son propre compte bancaire, le marchand 104 présente à l'intermédiaire financier 100, les jetons 107 correspondants aux transactions effectuées par ses clients. L'intermédiaire financier 100 vérifie la validité des transactions et effectue un rachat 108 des jetons présentés.

10 Selon une variante de réalisation de l'invention décrite à la figure 2, le marchand 204 comprend un lecteur de processeur sécurisé et le client comprend un processeur sécurisé amovible 202. Pour les transactions de macro et micropaiements, le processeur sécurisé amovible 202 est inséré dans le lecteur du marchand 204.

15 Les autres éléments et échanges effectués sont similaires aux éléments et échanges de la figure 1 précédemment décrite qui portent les mêmes numéros de référence et ne seront décrits davantage.

On note cependant que les échanges de données pour le macropaiement 105 et la création de jetons 106 se font par l'intermédiaire du marchand 204 qui reste transparent pour ces opérations.

20 La figure 3 illustre schématiquement un décodeur numérique multimédia 103 avec lecteur de processeur sécurisé tel qu'illustré en regard de la figure 1.

Le décodeur comprend reliés entre eux par un bus d'adresses et de données 303 :

- un processeur 302 ;
- 25 - un modem 301 ;
- un lecteur de processeur sécurisé 306
- une mémoire vive 305 ; et
- une mémoire non volatile 304.

30 Chacun des éléments illustrés en figure 3 est bien connu de l'homme du métier. Ces éléments communs ne sont pas décrits ici.

On observe cependant que le modem 301 est adapté à émettre et recevoir des signaux représentatifs de données multimédia en provenance d'un émetteur/récepteur extérieur non représenté tel que notamment un diffuseur de programmes de télévision, un lecteur de DVD, de CD audio ou CD-ROM. Le modem 301 est notamment adapté à mettre en forme les
35 signaux en provenance de l'extérieur sous forme de séquences binaires

exploitables par le processeur 302 et vice-versa. En outre, le modem 301 est adapté à émettre des données par exemple de type macro ou micropaiement vers un réseau auquel sont aussi connectés l'intermédiaire financier 100 et le marchand 104 ou à recevoir des données de ce réseau.

5 On observe en outre que le mot « registre » utilisé dans toute la description désigne dans chacune des mémoires mentionnées, aussi bien une zone de mémoire de faible capacité (quelques données binaires) qu'une zone mémoire de grande capacité (permettant de stocker un programme entier ou l'intégralité d'une séquence de données de transactions).

10 La mémoire vive 305 conserve des données, des variables et des résultats intermédiaires de traitement.

La mémoire non volatile 304 conserve dans des registres qui par commodité possèdent les mêmes noms que les données qu'ils conservent notamment le programme de fonctionnement du processeur 302
15 dans un registre « Prog » 306.

La figure 4 illustre schématiquement un décodeur numérique multimédia 103 avec processeur sécurisé fixe tel que mentionné en variante de la figure 1.

20 Hormis le processeur sécurisé fixe qui remplace un lecteur de processeur sécurisé amovible, les éléments illustrés en figure 4 sont similaires aux éléments de la figure 3 précédemment décrite qui portent les mêmes numéros de référence et ne seront décrits davantage.

On note que le décodeur 103 comprend reliés entre eux par un bus d'adresses et de données 303 :

- 25
- un processeur 302 ;
 - un modem 301 ;
 - un processeur sécurisé fixe 406 ;
 - une mémoire vive 305 ; et
 - une mémoire non volatile 304.

30 Le processeur sécurisé fixe 406 est adapté à gérer des transactions de micropaiement effectuées par le client 101.

La figure 5 illustre schématiquement un processeur sécurisé 500 tel que le processeur sécurisé 102 (respectivement 202) mentionné en regard de la figure 1 (respectivement 2).

35 Le processeur sécurisé 500 comprend reliés entre eux par un bus d'adresses et de données 503 :

- un processeur 502 ;
- un interface d'entrées/sorties 501 ; et
- une mémoire non volatile 504 de type EEPROM.

Chacun des éléments illustrés en figure 5 est bien connu de l'homme
5 du métier. Ces éléments communs ne sont pas décrits ici.

On observe cependant que l'interface 501 est adaptée à émettre et
recevoir des signaux représentatifs de données de transactions de macro ou
micropaiement multimédia en provenance d'un émetteur/récepteur extérieur
tel que notamment un intermédiaire financier ou un marchand.

10 La mémoire non volatile 504 conserve dans des registres qui par
commodité possèdent les mêmes noms que les données qu'ils conservent :

- le programme de fonctionnement du processeur 502 dans un registre
« *Prog* » 505 ,
- un compteur de jetons dans un registre *Tok* 506 ;
- 15 - une clé publique de signature d'intermédiaire financier dans un registre
BPubK 507 ;
- une clé publique dans un registre *PubK* 508 ;
- une clé privée dans un registre *PriK* 509 ; et
- dans un registre *Var* 510: des nombres ou variables utilisés provisoirement
20 pour certaines opérations, tels que des nombres *C*, *N*, *n* décrits par la
suite, ou des messages échangés.

La mémoire non volatile 504 est préférentiellement de type EEPROM
afin que l'on puisse mettre à jour et conserver des paramètres tels que le
contenu du porte-monnaie.

25 On note que les registres contenant le programme 505, le compteur de
jetons 506 et les clés 507, 508 et 509 sont par exemple initialisés lors de la
fabrication du processeur sécurisé et/ou lors de l'ouverture d'un compte chez
un intermédiaire financier.

30 La figure 6 illustre schématiquement un marchand 104 tel que décrit en
regard de la figure 1. Cette figure a été représentée uniquement dans la
phase de calcul.

Le marchand 104 comprend reliés entre eux par un bus d'adresses et
de données 603 :

- un processeur 602 adapté à la mise en œuvre de l'organigramme
35 décrit dans la figure 12;
- un modem 601 ;

- une mémoire non volatile 604;
- une mémoire vive 605 ; et
- une mémoire non volatile 613 de type EEPROM.

Chacun des éléments illustrés en figure 6 est bien connu de l'homme
5 du métier. Ces éléments communs ne sont pas décrits ici.

On observe cependant que l'interface 601 est adaptée à émettre et recevoir des signaux représentatifs de données de transactions de micropaiement en provenance d'un émetteur/récepteur extérieur tel que notamment un intermédiaire financier ou un client.

10 La mémoire non volatile 604 conserve dans des registres qui par commodité possèdent les mêmes noms que les données qu'ils conservent :

- le programme de fonctionnement du processeur 602 dans un registre « *Prog* » 607 ; et
- un registre « *IDM* » contenant l'identificateur du marchand 606 unique pour
15 l'intermédiaire financier.

La mémoire vive 605 conserve des données, des variables et des résultats intermédiaires de traitement, dans des registres de mémoire portant dans la description, les mêmes noms que les données dont ils conservent les valeurs. La mémoire vive 605 comprend notamment :

- 20 - dans un registre *Var* 612: des nombres ou variables utilisés provisoirement pour certaines opérations, tels que des nombres *n* décrits par la suite, ou des messages échangés.

La mémoire non volatile 613 de type EEPROM conserve dans des registres qui par commodité possèdent les mêmes noms que les données
25 qu'ils conservent :

- un registre « *TO* » 608 dans lequel est conservé le numéro de la transaction en cours ;
- un registre « *LTO* » 611 dans lequel est conservé le dernier numéro de transaction alloué ;
- 30 - un registre « *MpubK* » 609 dans lequel est conservée la clé publique du marchand ; et
- un registre « *MpriK* » 610 dans lequel est conservée la clé privée du marchand.

La figure 7 illustre schématiquement un marchand 204 tel que décrit en
35 regard de la figure 2. Cette figure a été représentée uniquement dans la phase de calcul.

Le marchand 204 comprend reliés entre eux par un bus d'adresses et de données 603 :

- un processeur 602 adapté à la mise en œuvre de l'organigramme décrit dans la figure 12;
- 5 - un modem 601 ;
- une mémoire non volatile 604 ;
- une mémoire vive 605 ;
- une mémoire non volatile 613 de type EEPROM ; et
- un lecteur de processeur sécurisé amovible 711.

10 Hormis la présence d'un lecteur de processeur sécurisé amovible, les éléments illustrés en figure 7 sont similaires aux éléments de la figure 6 précédemment décrite qui portent les mêmes numéros de référence et ne seront décrits davantage.

On note que le lecteur de processeur sécurisé 711 est adapté à lire un
15 processeur sécurisé amovible 202 décrit en regard de la figure 2 avec une réalisation 500 telle que décrite en regard de la figure 5.

On note que les flux de données de transactions vis-à-vis d'un client (respectivement d'un intermédiaire financier) se font alors par l'intermédiaire du lecteur de processeur sécurisé amovible 711 (respectivement du modem
20 601).

En considérant les figures 1, 2, 6 et 7, il est clair qu'un marchand peut effectuer des transactions avec un client distant et/ou avec un client de type processeur sécurisé amovible local.

25 La figure 8 illustre schématiquement un intermédiaire financier 100 tel que décrit en regard des figures 1 ou 2. Cette figure a été représentée uniquement dans la phase de calcul.

L'intermédiaire financier 100 comprend reliés entre eux par un bus d'adresses et de données 803 :

- 30 - un processeur 802 adapté à la mise en œuvre des organigrammes décrits dans les figures 13 ou 14;
- un modem 801 ;
- une mémoire non volatile 804 ;
- une mémoire vive 805 ; et
- une mémoire non volatile 810 de type EEPROM.

35 Chacun des éléments illustrés en figure 8 est bien connu de l'homme du métier. Ces éléments communs ne sont pas décrits ici.

On observe cependant que le modem 801 est adapté à émettre et recevoir des signaux représentatifs de données de transactions de macro ou micropaiement en provenance d'un émetteur/récepteur extérieur tel que notamment un marchand ou un client.

5 La mémoire non volatile 804 conserve dans des registres qui par commodité possèdent les mêmes noms que les données qu'ils conservent :

- le programme de fonctionnement du processeur 602 dans un registre « *Prog* » 806 , et
- un registre « *BpriK* » 808 dans lequel est conservée la clé privée de l'intermédiaire financier qui sert à générer les certificats pour les autres clés publiques du système.

10 La mémoire non volatile 810 de type EEPROM conserve dans des registres qui par commodité possèdent les mêmes noms que les données qu'ils conservent, notamment :

- 15 - un registre « *MLTO* » 807 dans lequel est conservé le numéro de la dernière transaction valide de chaque marchand connu de l'intermédiaire financier.

20 La mémoire vive 805 conserve des données, des variables et des résultats intermédiaires de traitement, dans des registres de mémoire portant dans la description, les mêmes noms que les données dont ils conservent les valeurs. La mémoire vive 805 comprend notamment :

- dans un registre *Var* 809: des nombres ou variables utilisés provisoirement pour certaines opérations, tels que des nombres *LTV*, *n* décrits par la suite, ou des messages échangés.

25 La figure 9 détaille un protocole de chargement de jetons sur un processeur sécurisé destinés à des transactions de micropaiement ainsi que les flux de données correspondants.

Le chargement de jetons fait intervenir :

- 30 - un processeur sécurisé 900 tel que le processeur 102 décrit en regard de la figure 1 avec une réalisation 500 telle que décrite en regard de la figure 5 ;
- un décodeur multimédia 901 tel que le décodeur 103 décrit en regard de la figure 1 ; et
- 35 - un intermédiaire financier 902 tel que l'intermédiaire financier 100 décrit en regard de la figure 1.

La procédure de chargement de jetons se fait en deux étapes :

- une étape de macropaiement où un client achète des jetons (monnaie électronique) à l'intermédiaire financier. Cette étape ne concerne pas directement l'invention. L'homme du métier l'implante par exemple en utilisant le protocole de macropaiement « SET » (acronyme anglais de « Secure Electronic Transactions ») ; et
- une étape d'authentification et de chargement durant laquelle le compteur d'argent du processeur sécurisé est incrémenté du montant de la monnaie électronique achetée.

La procédure de chargement de jetons débute par l'envoi d'un message de début de chargement de jetons 903 du décodeur 901 vers le processeur sécurisé 900. Puis, le processeur sécurisé 900 génère un nombre C aléatoire qu'il transmet au décodeur 901. Ce nombre C est utilisé pour empêcher les attaques de type dictionnaire contre le processeur sécurisé qui consisteraient à enregistrer toutes les valeurs possibles d'une fonction de signature par l'intermédiaire financier $Sign(C,N)$ qui est utilisée par la suite. Le nombre C doit être suffisamment grand (par exemple un nombre de 64 bits ou éléments binaires) pour rendre inutiles des attaques de ce type.

Ensuite, le décodeur contacte l'intermédiaire financier 902 pour acheter N jetons avec un message 905 contenant les valeurs de N et C .

Une transaction de macropaiement 906 s'effectue alors entre le décodeur et l'intermédiaire financier.

Puis, l'intermédiaire financier 902 signe le message contenant C et N à l'aide de sa clé privée $BPriK$ 808 en utilisant des schémas de signature standard PKCS#1 (standard du laboratoire RSA publié dans le document « PKCS#1 v2.1 :RSA Cryptography standard, RSA Laboratories – Draft 1 – September 17, 1999 ») pour obtenir un message signé ou signature « $Sign(C,N)$ » 907 qu'il transmet au décodeur 901. Cela permet au décodeur et au processeur sécurisé qui vont recevoir ce message d'authentifier que les jetons proviennent bien de l'intermédiaire financier 902. La fonction de signature est basée sur un algorithme de cryptage asymétrique. On pourra se référer à l'ouvrage « Applied Cryptography » écrit par de B. Schneier chez l'éditeur Wesley&Sons en 1996 pour la mise en œuvre des méthodes de cryptage asymétriques.

Ensuite, le décodeur 901 transmet au processeur sécurisé 900 un message 908 contenant la valeur de N ainsi que la signature $Sign(C,N)$.

Le processeur sécurisé 900 vérifie à l'étape 909 l'authenticité de ce message en vérifiant la signature $\text{Sign}(C,N)$ à l'aide de la clé publique de l'intermédiaire financier $BP_{\text{Pub}K}$ contenu dans le registre 507.

5 La clé privée de l'intermédiaire financier $BP_{\text{Pri}K}$ et sa clé publique $BP_{\text{Pub}K}$ de signature seront d'une taille suffisamment élevée pour rendre toute attaque impossible. Elles pourront par exemple contenir 160 bits ou éléments binaires.

Lorsque le message est authentifié, au cours d'une étape 910, le compteur de monnaie Tok mémorisé dans le registre 506 est incrémenté de la
10 valeur de N .

On note que dans une réalisation telle que décrite en regard de la figure 2, le processeur sécurisé 202 et le marchand 204 remplacent pour certaines opérations le décodeur 901 dans le protocole décrit en regard de la figure 9.

15 La figure 10 présente un protocole de dépense de jetons sur un processeur sécurisé.

Une dépense de jetons fait intervenir :

- un processeur sécurisé 900 tel que le processeur 102 décrit en regard de la figure 1 avec une réalisation 500 telle que décrite en
20 regard de la figure 5 ;
- un décodeur multimédia 901 tel que le décodeur 103 décrit en regard de la figure 1 ; et
- un marchand 902 tel que le marchand 104 décrit en regard de la figure 1.

25 Une transaction de micropaiement débute par une requête 1001 d'achat d'une marchandise ou d'un service valant n jetons effectuée par le décodeur 901 vers le marchand 902.

A la réception de cette requête, le marchand génère un numéro de transaction TO conservé dans le registre 608 suivant un procédé décrit en
30 regard de la figure 12. Le marchand 902 transmet alors au décodeur 901 un message 1002 contenant son identificateur IDM conservé dans le registre 606 et la valeur de TO .

Puis, le décodeur 901 communique la valeur de n , le numéro de transaction TO et l'identificateur du marchand IDM regroupés dans un
35 message 1003, au processeur sécurisé 900.

Après avoir vérifié que le compteur *Tok* contient suffisamment de jetons, c'est à dire que *Tok* est supérieur ou égal à *n*, le processeur sécurisé décrémente le compteur de jetons *Tok* de la valeur *n* au cours d'une étape 1004.

5 Ensuite, le processeur sécurisé signe un message contenant *n*, *TO* et *IDM* pour former un message noté *Sign(n,TO,IDM)* avec un algorithme asymétrique et sa propre clé privée *PriK* conservée dans le registre 509. Puis, un message (1005,1006) contenant *TO*, *Sign(n,TO,IDM)* et la clé publique du processeur sécurisé *PubK* 508 est transmis vers le marchand 902 à travers le
10 décodeur 901. On note que le numéro de transaction *TO* a pu être mémorisé par le décodeur 901 et qu'ainsi le processeur sécurisé 900 n'est pas obligé de transmettre *TO* au décodeur 901. La clé publique du processeur sécurisé *PubK* est elle même composée de deux entités :

- 15 - une clé publique de signature notée *PubK.key* qui est utilisée pour l'algorithme de signature présent sur le processeur sécurisé ; et
- la signature de la clé publique de signature *PubK.key* notée *PubK.Sign* qui a été obtenue avec la clé privée de l'intermédiaire financier *BPriK*.

20 Ainsi, le marchand vérifie la validité de la transaction en vérifiant d'une part la validité du certificat de clé publique en utilisant la clé publique de l'intermédiaire financier *BPubK* et d'autre part en vérifiant la signature du triplet (*n,TO,IDM*) avec la clé publique de signature du processeur sécurisé *PubK.key*. On note aussi, que l'intermédiaire financier peut ultérieurement effectuer les mêmes vérifications.

25 On note qu'une opération de validation du marchand peut être insérée avant toute transaction. Elle peut par exemple consister en une émission d'un certificat du marchand vers un client.

 On note que dans une réalisation telle que décrite en regard de la figure 2, le processeur sécurisé 202 et le marchand 204 remplacent pour
30 certaines opérations le décodeur 901 dans le protocole décrit en regard de la figure 10.

 La figure 11 présente un protocole de rachat des jetons au marchand suite à une ou plusieurs transactions effectuées par un ou plusieurs clients.

 Le rachat de jetons fait intervenir :

- 35 - un marchand 902 tel que le marchand 104 ou 204 décrit en regard des figures 1 ou 2 ; et

- un intermédiaire financier 1101 tel que l'intermédiaire financier 100 décrit en regard de la figure 1.

Si une transaction est reconnue comme correcte, l'intermédiaire financier peut rembourser le marchand. On note que le remboursement des transactions relatives à un marchand donnée (ou rachat de jetons au marchand) durant une période peut se faire en une seule fois pour réduire les coûts. L'intermédiaire financier peut aussi réduire ses coûts en ne vérifiant complètement que certaines transactions. En cas de détection d'une transaction non valide, l'intermédiaire financier pourra vérifier toutes les transactions effectuées par le marchand correspondant. Le procédé de vérification pourra être optimisé pour maximiser la rentabilité de l'intermédiaire financier.

L'opération de rachat des jetons est initiée par le marchand 902 qui, au cours d'une étape 1102, construit un message signé noté *MSign* obtenu en signant avec sa propre clé privée *MPriK* conservée dans le registre 610, un quadruplet constitué de la valeur de la transaction n , du numéro de transaction TO , de l'identificateur du marchand IDM et du message signé $Sign(n, TO, IDM)$ émis par le processeur sécurisé concerné par la transaction.

Puis, le marchand 902 envoie à l'intermédiaire financier 1101 un message 1103 de demande de remboursement de transaction comprenant la valeur de la transaction n , le numéro de transaction TO , son identificateur IDM , le message signé $Sign(n, TO, IDM)$, le message signé *MSign* et la clé publique du marchand *MPubK* 609.

L'intermédiaire financier 1101 peut alors vérifier la transaction selon l'un des algorithmes décrits en regard des figures 13 ou 14 au cours d'une étape 1104.

En figure 12, qui présente une génération de numéros de transactions par un marchand 104 ou 204 tel qu'illustré en regard des figures 1 ou 2, on observe qu'après une opération d'initialisation 1200 au cours de laquelle les registres de la mémoire vive 605 et de la mémoire non volatile 613 de type EEPROM sont initialisés, au cours d'une opération d'attente 1201, le processeur 602 attend de recevoir puis reçoit une nouvelle requête de transaction.

Puis, au cours d'une opération d'allocation 1202, le processeur 602 alloue un numéro de transaction TO puis mémorise ce numéro dans un registre 611 de dernier numéro de transaction mémorisé LTO .

Ensuite, au cours d'une opération d'attente 1203, le processeur 602 attend de recevoir puis reçoit une requête de transaction.

Puis, au cours d'une opération d'allocation 1204, le processeur 602 alloue un numéro de transaction *TO* qui suit selon un ordre préétabli le dernier
5 numéro mémorisé *LTO* dans le registre 611. L'ordre est établi notamment par le marchand, un intermédiaire financier ou un opérateur technique.

Selon le mode préféré de réalisation, cet ordre préétabli sera l'ordre croissant des entiers naturels. *TO* sera alors obtenu par incrément d'une unité de la valeur de *LTO*.

10 Selon une variante, cet ordre préétabli sera l'ordre décroissant des entiers naturels ou un ordre quelconque qui par exemple dépend du mode de représentation de ces entiers.

Selon une autre variante, le numéro de transaction correspond à une heure et/ou une date. L'ordre préétabli est alors un ordre chronologique.

15 Selon le mode préféré de réalisation, le système est conçu pour que *TO* n'atteigne jamais une valeur maximale définie par l'ordre préétabli dans un délai raisonnable.

Selon une variante, le nombre de valeurs possibles que peut prendre *TO* est limité et lorsque *TO* atteint une valeur donnée de fin, la valeur suivante
20 est une autre valeur donnée dite de début. Ainsi, l'ordre préétabli à prendre en compte est un ordre en boucle. Dans le cas, par exemple où on considère un compteur pouvant aller de 0 à 255, avec l'ordre naturel des entiers croissants, après la valeur 255, on pourra attribuer la valeur 0 à *TO*. Pour comparer deux nombres, on considère alors une fenêtre glissante de
25 comparaison par exemple de taille 4. Ainsi, dans la fenêtre glissante constituée des nombres 12, 13, 14 et 15, le nombre 14 est supérieur aux nombres 12 et 13 et inférieur au nombre 15. Lorsqu'une fenêtre glissante comprend la valeur de fin ou de début, on veillera à considérer l'ordre d'attribution des numéros. Ainsi, dans la fenêtre glissante constituée des
30 nombres 254, 255, 0 et 1, le nombre 0 est supérieur selon l'ordre en boucle préétabli aux nombres 254 et 255 et inférieur au nombre 1.

Les variantes d'ordre préétabli décrites ici ne sont pas limitatives et il existe de nombreuses possibilités pour l'ordre préétabli. D'une manière générale, cet ordre peut être établi notamment par le marchand, un
35 intermédiaire financier ou un opérateur technique. Si ce n'est pas le marchand 104 ou 204 qui a établi l'ordre de numérotation des transactions, les

paramètres de cet ordre préétabli sont transmis au marchand 104 ou 204 au préalable ou lors de l'opération d'allocation 1202 par un moyen quelconque connu de l'homme du métier.

5 Suite à l'opération d'allocation 1204, l'opération d'attente 1203 est réitérée.

En figure 13, qui présente une validation de transactions par un intermédiaire financier 100 tel qu'illustré en regard de la figure 8, on observe qu'après une opération d'initialisation 1300 au cours de laquelle les registres de la mémoire vive 805 et de la mémoire non volatile 810 de type EEPROM
10 sont initialisés, au cours d'une opération d'attente 1301 le processeur 802 attend de recevoir puis reçoit une requête de remboursement de transaction émise par un marchand 104 ou 204. Cette requête comprend notamment la valeur de la transaction n , un numéro de transaction TO , un identificateur du marchand IDM , un message signé $Sign(n, TO, IDM)$ par un client, un message
15 signé $MSign$ par le marchand et la clé publique du marchand $MPubK$.

Au cours d'un test 1302, le processeur 802 teste s'il s'agit d'une première requête valide issue du marchand M considéré, identifié grâce à l'identificateur IDM présent dans la requête de remboursement.

Dans la négative, le processeur effectue un test 1303 au cours duquel il
20 vérifie si le numéro TO de la transaction considérée est supérieur à un dernier numéro de transaction valide effectuée par le marchand considéré, ce dernier numéro étant conservé dans un registre $MLTO(M)$ 807. On suppose que le processeur effectue ce test en considérant le même ordre préétabli que celui utilisé par le marchand lors de l'allocation des numéros de transactions et qui
25 a été décrit en détail en regard de la figure 12. Si ce n'est pas l'intermédiaire financier 100 qui a établi l'ordre de numérotation des transactions par le marchand M , les paramètres de cet ordre préétabli sont transmis à l'intermédiaire financier 100, au préalable ou lors du test 1303 par un moyen quelconque connu de l'homme du métier.

30 Lorsque le résultat de l'un des tests 1302 ou 1303 est positif, le processeur 802 effectue un test de signature de la transaction incluant notamment un test de $Sign$ et/ou de $MSign$ tels que reçu par l'intermédiaire financier.

Lorsque la signature testée est valide, le processeur 802 effectue une
35 mise à jour du registre de dernier numéro de transaction enregistré pour le marchand $MLTO(M)$ en mémorisant dans ce registre la valeur du numéro de

transaction *TO* et l'intermédiaire financier peut rembourser le marchand d'un montant n spécifié par la requête.

Lorsque le résultat de l'un des tests 1303 ou 1304 est négatif, le processeur 802 rejette la transaction au cours d'une opération 1306.

5 A la suite de l'une des opérations 1305 ou 1306, l'opération d'attente 1301 est réitérée.

La figure 14 présente un organigramme de validation de transactions par l'intermédiaire financier selon une variante où la vérification des signatures est facultative. Les autres opérations effectuées sont similaires aux
10 opérations de la figure 13 précédemment décrite qui portent les mêmes numéros de référence et ne seront pas décrits davantage.

On observe que lorsque le résultat de l'un des tests 1302 ou 1303 est positif on effectue un test pour déterminer si une vérification de signature est requise. Au cours de ce test, on considère un indice de fiabilité du marchand.
15 Si cet indice est inférieur à un seuil minimal de fiabilité, la signature est vérifiée systématiquement. Si cet indice est supérieur à ce seuil minimal de fiabilité, la signature ne sera pas systématiquement vérifiée ; elle sera par exemple vérifiée après un tirage pseudo aléatoire dont la probabilité d'issue positive dépend de l'indice de fiabilité du marchand ou selon une fréquence
20 qui est aussi dépendante de l'indice de fiabilité du marchand.

Lorsque le test 1407 requiert une vérification de signature, le test 1304 décrit précédemment est effectué.

Lorsque le test 1304 est positif, le processeur 802 met à jour l'indice de fiabilité du marchand qui est augmenté et un registre *LTV* de dernière
25 transaction validée en y enregistrant le numéro de transaction *TO* lors d'une opération de mise à jour 1408.

Lorsque le test 1407 ne requiert pas de vérification de signature ou après l'opération de mise à jour 1408, le processeur 802 effectue l'opération 1305 précédemment décrite.

30 Lorsque le résultat du test de signature 1304 est négatif, le processeur 802 effectue une mise à jour de l'indice de fiabilité du marchand en la diminuant lors d'une opération 1409.

Puis, à l'issue d'un test 1303 négatif ou d'une opération 1409, la transaction est rejetée au cours d'une opération 1306.

A la suite de cette opération de rejet 1306, au cours d'une opération 1410, le processeur 802 effectue une opération de vérification de toutes les transactions effectuées par le marchand considéré *M*,

- dont la signature n'a pas été validée et
- 5 - dont le numéro *TO* est supérieur au dernier numéro *LTV* de transaction dont la signature a été validée et/ou au dernier numéro de transaction ayant reçu une acceptation de paiement pour remboursement. (On note que l'acceptation de paiement n'est pas nécessairement immédiate après la validation d'une transaction,
- 10 mais se fait par exemple à une date précise chaque mois).

Chaque transaction dont la signature n'est pas validée et qui avait été validée dans un premier temps par un simple test de numéro de transaction est finalement rejetée. Ensuite, une mise à jour de l'indice de fiabilité du marchand est effectuée.

15 A la suite de l'une des opérations 1305 ou 1410, l'opération d'attente 1301 est réitérée.

Bien entendu, l'invention n'est pas limitée aux exemples de réalisation mentionnés ci-dessus.

20 En particulier, l'homme du métier pourra apporter toute variante dans la définition des types de client, de marchand ou d'intermédiaire financier lorsque le marchand applique un procédé de gestion des transactions avec une allocation des numéros de transactions *TO* et/ou un intermédiaire financier valide une transaction numérotée ainsi telle que décrite dans le mode préféré de réalisation.

25 On note que l'architecture du système ne se limite pas à une architecture triangulaire client, marchand, intermédiaire financier mais s'étend à tout type d'architecture comprenant au moins un client, au moins un marchand et au moins un intermédiaire financier reliés entre eux. On peut ainsi considérer plusieurs clients pouvant effectuer des transactions avec

30 plusieurs marchands, chacun des marchands étant reliés à un ou plusieurs intermédiaires financiers, chacun des clients pouvant effectuer des macropaiements avec un ou plusieurs intermédiaires financiers qui ne sont pas nécessairement les mêmes que ceux de chacun des marchands.

35 On notera que l'invention ne se limite pas à une implantation purement matérielle mais qu'elle peut aussi être mise en œuvre sous la forme d'une séquence d'instructions d'un programme informatique ou toute forme mixant

une partie matérielle et une partie logicielle. Dans le cas où l'invention est implantée partiellement ou totalement sous forme logicielle, la séquence d'instructions correspondante pourra être stockée dans un moyen de stockage amovible (tel que par exemple une disquette, un CD-ROM ou un 5 DVD-ROM) ou non, ce moyen de stockage étant lisible partiellement ou totalement par un ordinateur ou un microprocesseur.

REVENDICATIONS

1. Procédé de gestion de transaction de micropaiement, entre un marchand (104) et au moins un client (101, 201) caractérisé en ce que, à chaque
5 nouvelle transaction,
- ledit marchand (104) alloue (1204) un nouveau numéro de transaction (TO) qui suit selon un ordre préétabli de numérotation un dernier numéro mémorisé (LTO) et
- ledit marchand (104) met à jour (1204) un registre de dernier numéro
10 mémorisé (LTO) en enregistrant ledit nouveau numéro de transaction (TO),
chaque dit numéro de transaction (TO) étant susceptible d'être vérifié par un intermédiaire financier (100).
- 15 2. Procédé de gestion de transaction de micropaiement selon la revendication 1, caractérisé en ce qu' au moins un client (101, 201) parmi lesdits clients est un terminal (103) multimédia numérique et/ou analogique.
- 20 3. Procédé de gestion de transaction de micropaiement selon la revendication 2, caractérisé en ce que ledit terminal (103) multimédia comprend au moins un processeur sécurisé fixe (102, 406) ou amovible (102, 500) nécessaire à la mise en œuvre desdites transactions de micropaiement.
- 25 4. Procédé de gestion de transaction de micropaiement selon l'une quelconque des revendications 1 à 3, caractérisé en ce que ledit marchand (104, 204) est équipé d'un lecteur (711) de processeur sécurisé amovible.
- 30 5. Procédé de gestion de transaction de micropaiement selon la revendication 4, caractérisé en ce qu'au moins un client (101, 201) parmi lesdits clients est un processeur sécurisé amovible (102,500) lisible par ledit lecteur (711) de processeur sécurisé amovible dudit marchand (104, 204).
- 35 6. Procédé de gestion de transaction de micropaiement entre un client (101, 201) et un marchand (104) par un intermédiaire financier (100), caractérisé en ce que

pour un premier ensemble d'au moins une transaction réalisée par ledit marchand (104) et possédant un numéro de transaction (*TO*) alloué par ledit marchand (104), ledit intermédiaire financier (100) effectue pour chaque transaction dudit premier ensemble

- 5 - au cours d'une première étape, une opération de vérification (1303) de ladite transaction consistant à déterminer si ledit numéro de transaction (*TO*) suit selon un ordre préétabli un dernier numéro de transaction enregistré (*MLTO(M)*) puis
- au cours d'une deuxième étape,
- 10 - lorsque le résultat de ladite opération de vérification est négatif, une opération (1306) de rejet de ladite transaction ;
- et lorsque le résultat de ladite opération de vérification est positif, une opération d'enregistrement (1305) dudit numéro de transaction (*TO*) en tant que dernier numéro de transaction (*MLTO(M)*) pour ledit marchand.
- 15

7. Procédé de gestion de transaction de micropaiement selon la revendication 6, caractérisé en ce que l'opération de vérification de ladite transaction comprend en outre une opération de vérification (1304) de signature de ladite transaction.

20

8. Procédé de gestion de transaction de micropaiement selon la revendication 7, caractérisé en ce que l'opération de vérification de ladite transaction est effectuée selon (1407) un indice de fiabilité dudit marchand.

25

9. Procédé de gestion de transaction de micropaiement selon la revendication 8, caractérisé en ce que la vérification de signature (1304) de ladite transaction est effectuée

- systématiquement si ledit indice de fiabilité dudit marchand est inférieur à un seuil ;
- 30 - non systématiquement si ledit indice de fiabilité dudit marchand est supérieur au dit seuil.

10. Procédé de gestion de transaction de micropaiement selon la revendication 9, caractérisé en ce que lorsque le résultat de l'opération de vérification de signature (1304) de ladite transaction est négatif, le procédé

35

comprend en outre une opération (1410) de vérification des signatures d'un deuxième ensemble de transactions.

5 **11.** Procédé de gestion de transaction de micropaiement selon la revendication 10, caractérisé en ce que ledit deuxième ensemble de transactions comprend toutes les transactions présentées par ledit marchand audit intermédiaire financier depuis une transaction de référence et dont la signature n'a pas déjà été vérifiée.

10 **12.** Procédé de gestion de transaction de micropaiement selon la revendication 11, caractérisé en ce que ladite transaction de référence est :

- la dernière transaction ayant reçu une acceptation de paiement ; et/ou
- la dernière transaction (LTV) précédant ladite transaction de micropaiement dont la signature a été vérifiée.

15 **13.** Procédé de gestion de transaction de micropaiement selon l'une quelconque des revendications 8 à 12, caractérisé en ce que ledit intermédiaire financier est susceptible de mettre à jour la fiabilité dudit marchand en fonction du résultat d'au moins une desdites vérifications de signature (1304).

20

14. Procédé de gestion de transaction de micropaiement selon l'une quelconque des revendications 1 à 13, caractérisé en ce que ledit ordre préétabli a été établi par ledit marchand (104) ou ledit intermédiaire financier (100) ou un opérateur technique.

25

15. Procédé de gestion de transaction de micropaiement selon l'une quelconque des revendications 1 à 14, caractérisé en ce que ledit ordre préétabli est

30

- l'ordre naturel des entiers croissants ; et/ou
- un ordre chronologique de type heure et/ou date.

16. Procédé de gestion de transaction de micropaiement selon l'une quelconque des revendications 1 à 15, caractérisé en ce que ledit ordre préétabli est un ordre en boucle.

35

17. Système caractérisé en ce qu'il comprend des moyens adaptés à la mise en œuvre d'un procédé de gestion de transaction de micropaiement selon l'une quelconque des revendications 1 à 16.

- 5 18. Dispositif de gestion de transaction de micropaiement, entre ledit dispositif et au moins un client, caractérisé en ce qu'il comprend pour chaque nouvelle transaction,
- un moyen d'allocation de nouveau numéro de transaction (*TO*) qui suit selon un ordre préétabli de numérotation un dernier numéro mémorisé
 - 10 (*LTO*) ; et
 - un moyen de mise à jour dudit registre de dernier numéro mémorisé (*LTO*) ledit moyen de mise à jour enregistrant ledit nouveau numéro de transaction ;
- chaque dit numéro de transaction (*TO*) étant susceptible d'être vérifié par un
- 15 intermédiaire financier (100).

19. Dispositif de gestion de transaction de micropaiement entre un client (101, 201) et un marchand (104), caractérisé en ce que
- pour un premier ensemble de transactions réalisées par ledit marchand (104)
- 20 et possédant un numéro de transaction (*TO*) alloué par ledit marchand (104), ledit dispositif comprend pour chaque transaction dudit premier ensemble
- un moyen de vérification de ladite transaction adapté à déterminer si ledit numéro de transaction (*TO*) suit selon un ordre préétabli un dernier numéro de transaction enregistré (*MLTO(M)*) ;
 - 25 - lorsque le résultat de ladite opération de vérification est négatif, un moyen de rejet de ladite transaction ;
 - et lorsque le résultat de ladite opération de vérification est positif, un moyen d'enregistrement dudit numéro de transaction (*TO*) en tant que dernier numéro de transaction (*MLTO(M)*) pour ledit marchand (104).

- 30 20. Terminal numérique multimédia, caractérisé en ce qu'il comprend au moins un processeur sécurisé fixe (102, 406) ou amovible (102, 500) et en ce que ledit processeur sécurisé (102, 406, 500) est adapté à effectuer des transactions de micropaiements en tant que client (101,201).

35

21. Terminal numérique multimédia selon la revendication 20 caractérisé en ce qu'il est un décodeur numérique multimédia (103).

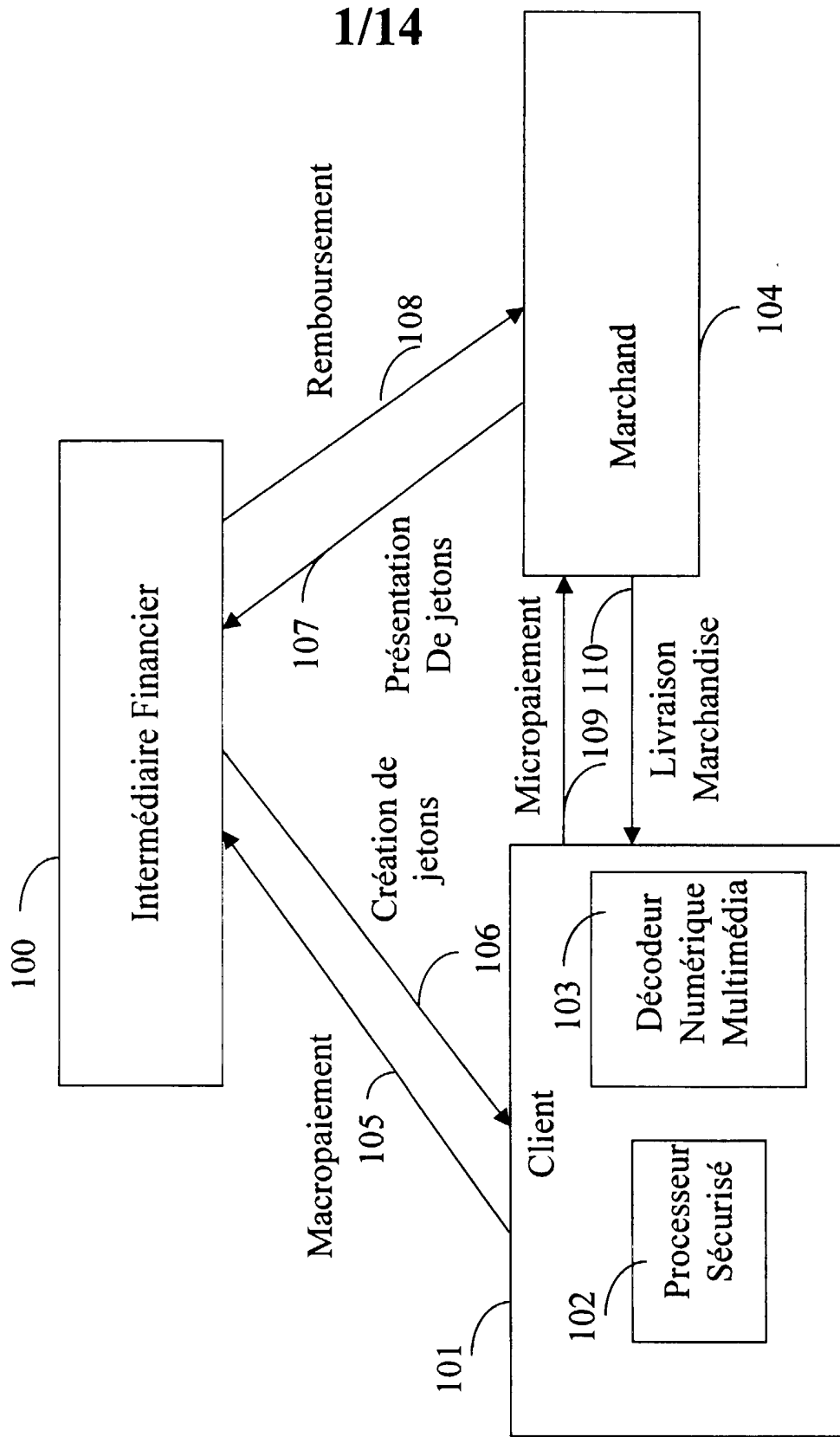


Fig. 1

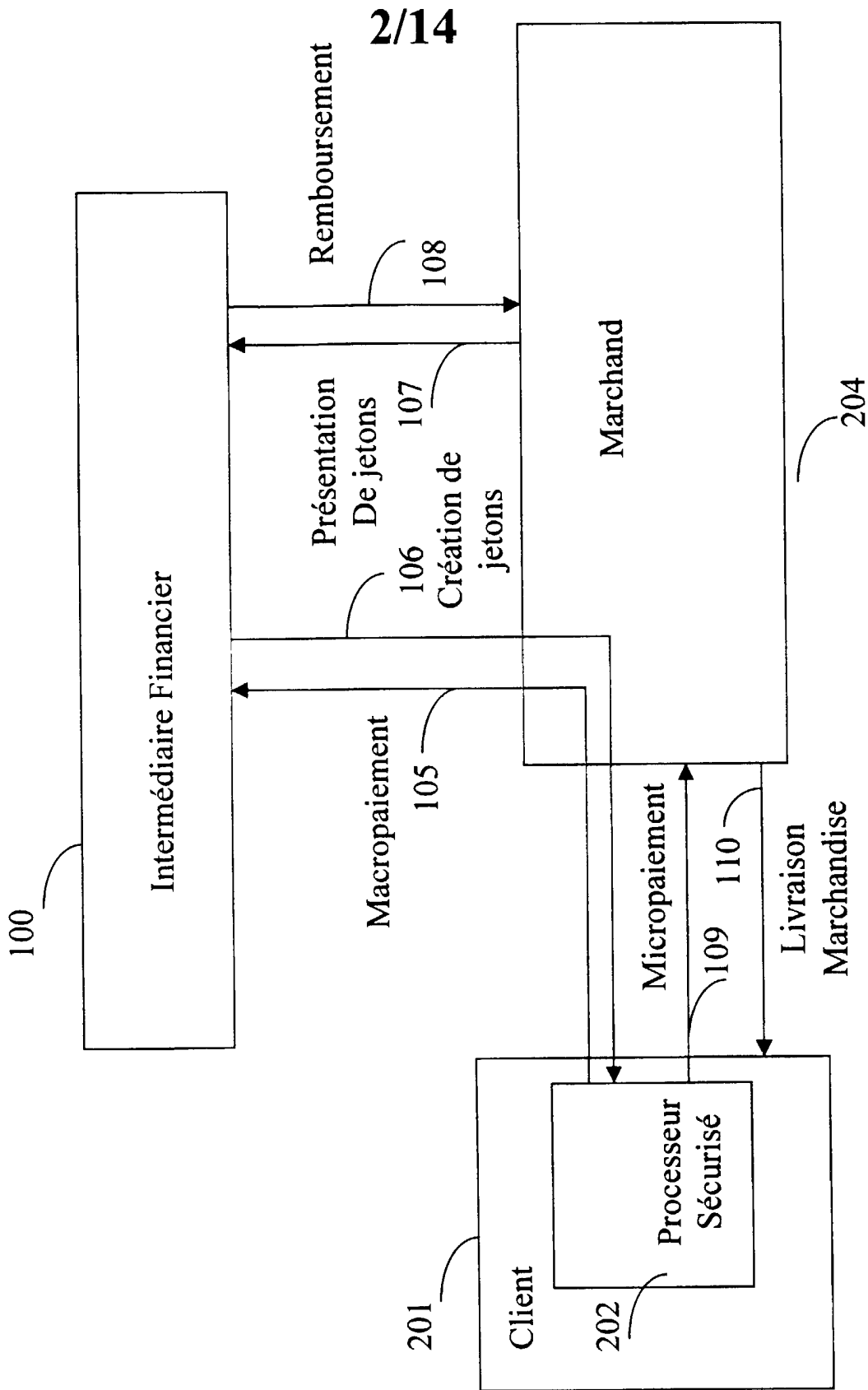


Fig. 2

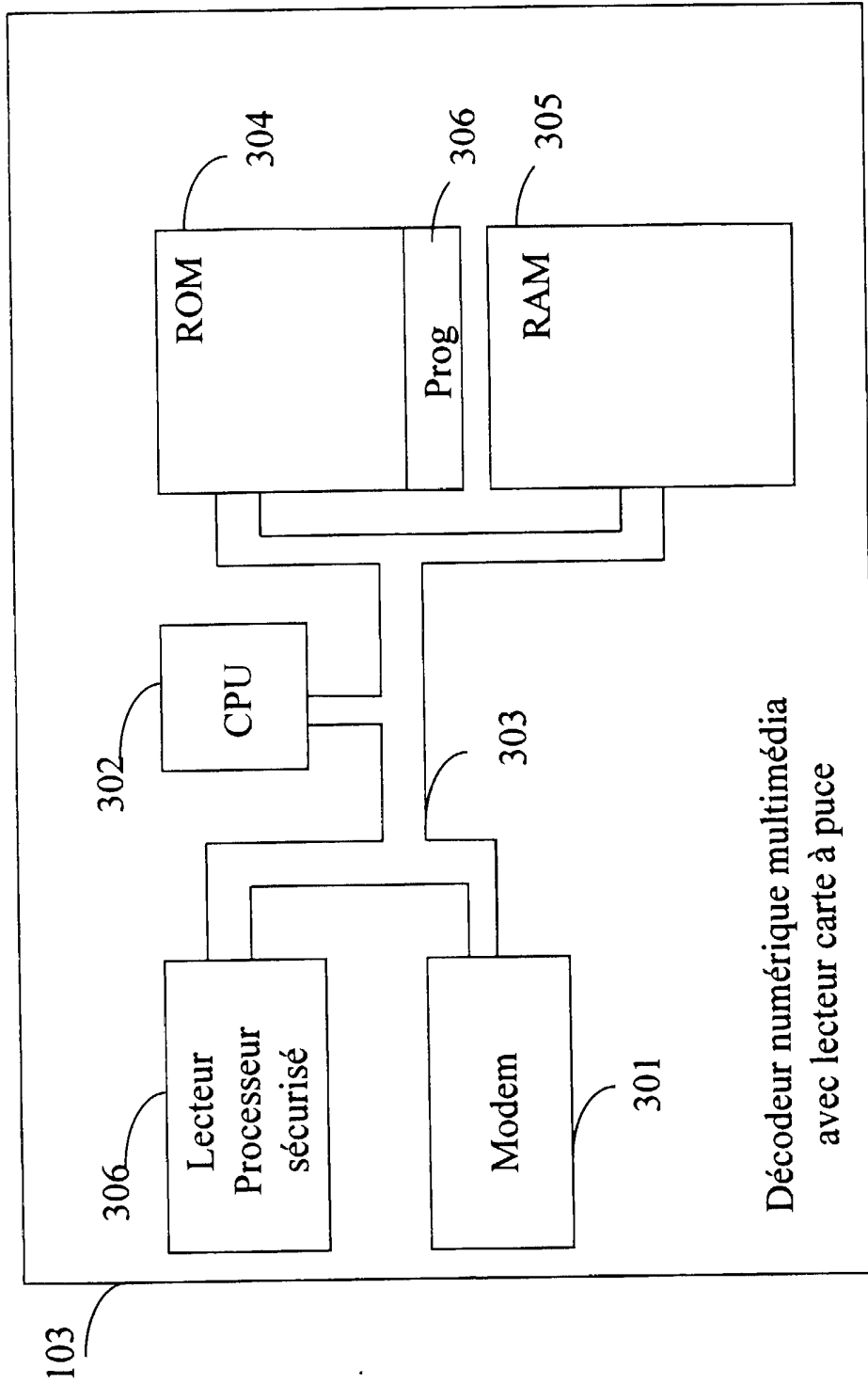


Fig. 3

4/14

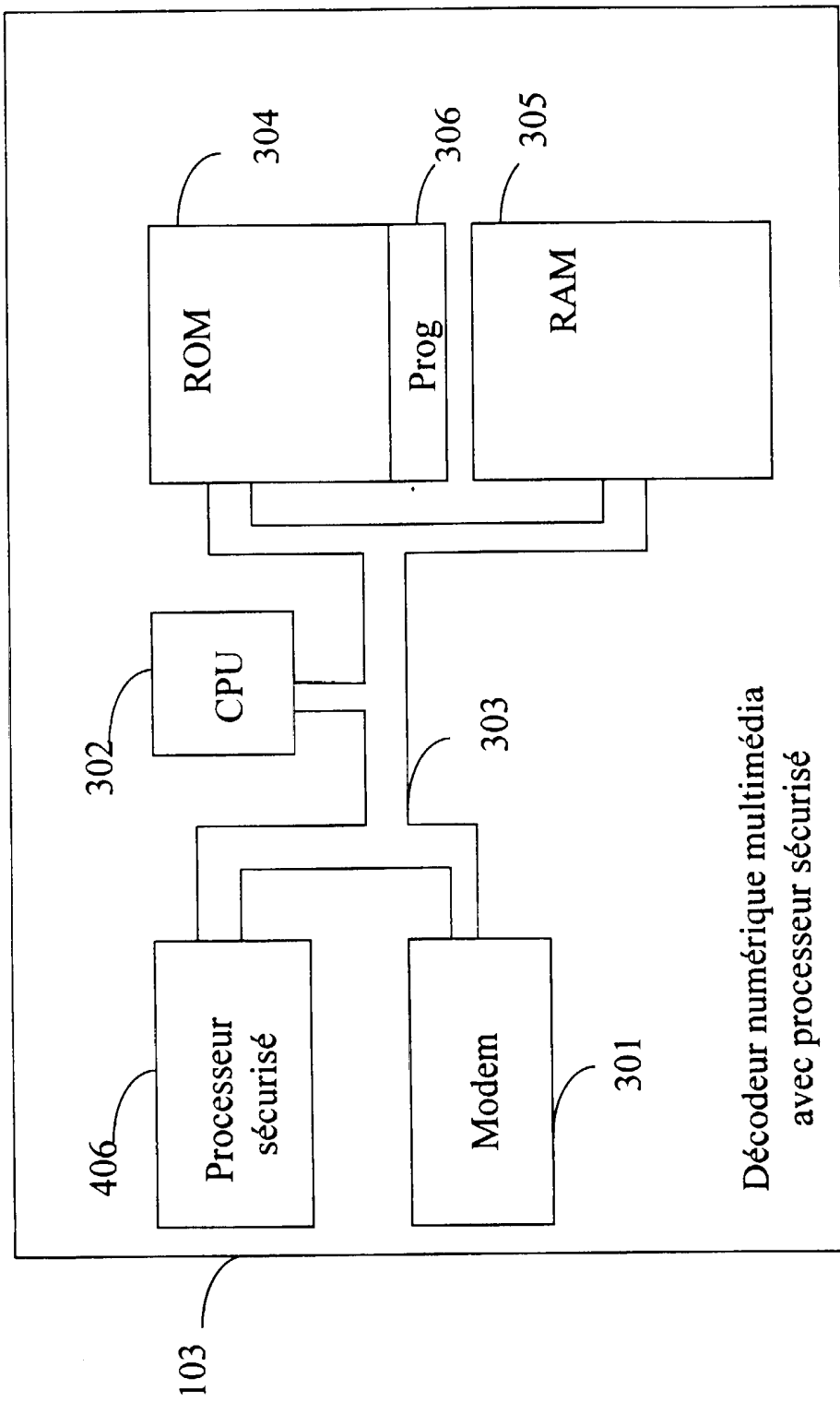


Fig. 4

5/14

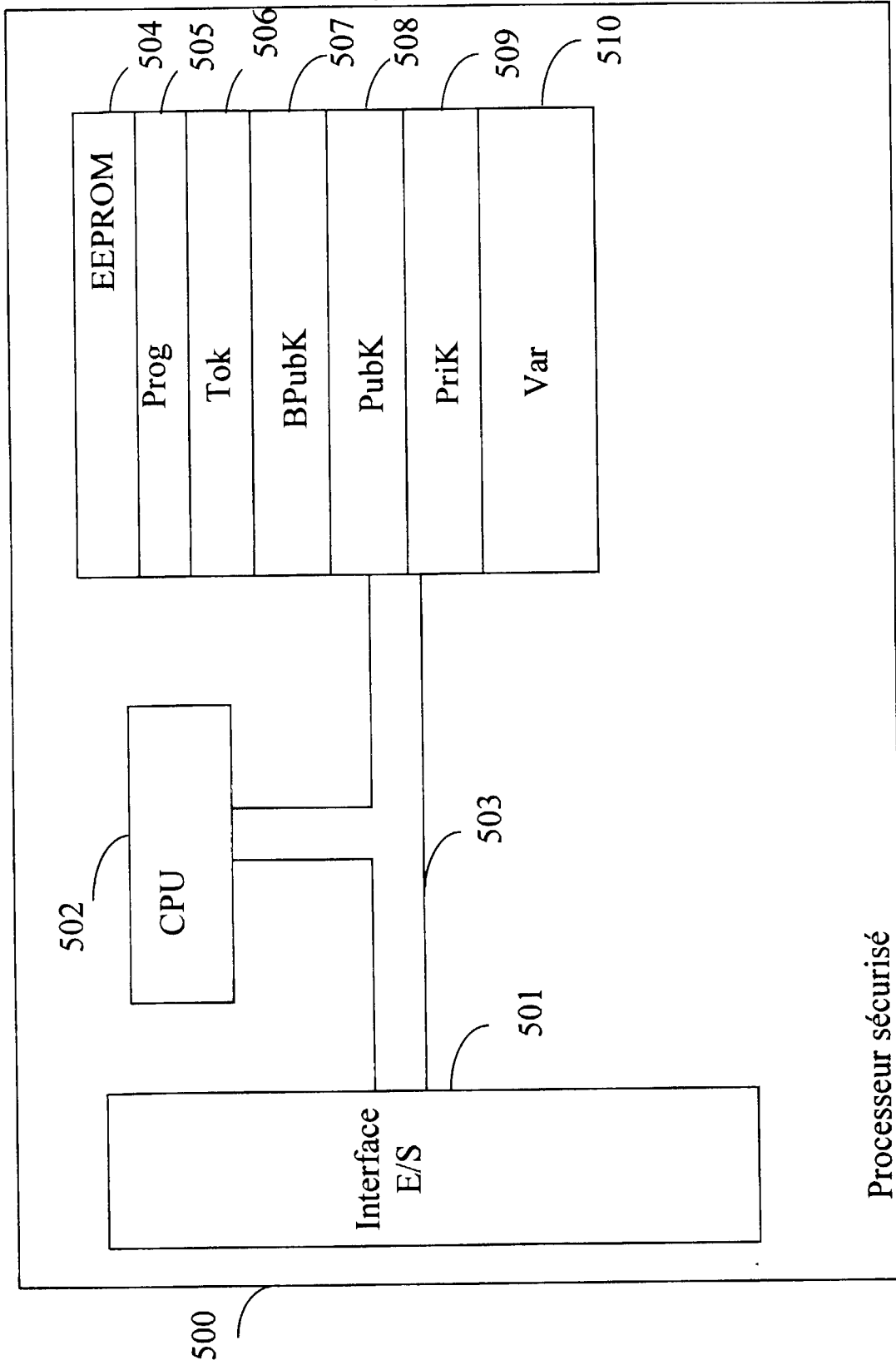


Fig. 5

6/14

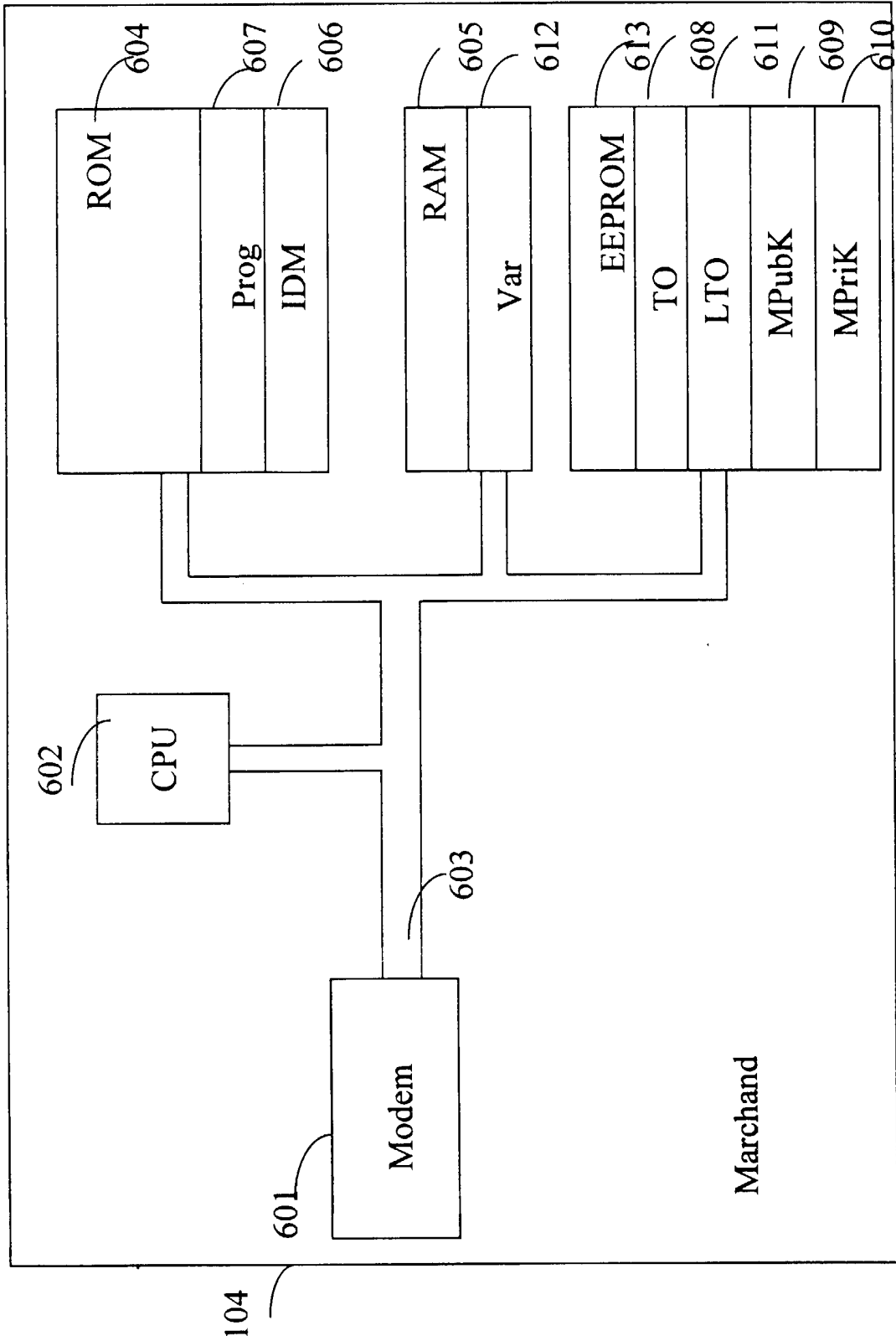


Fig. 6

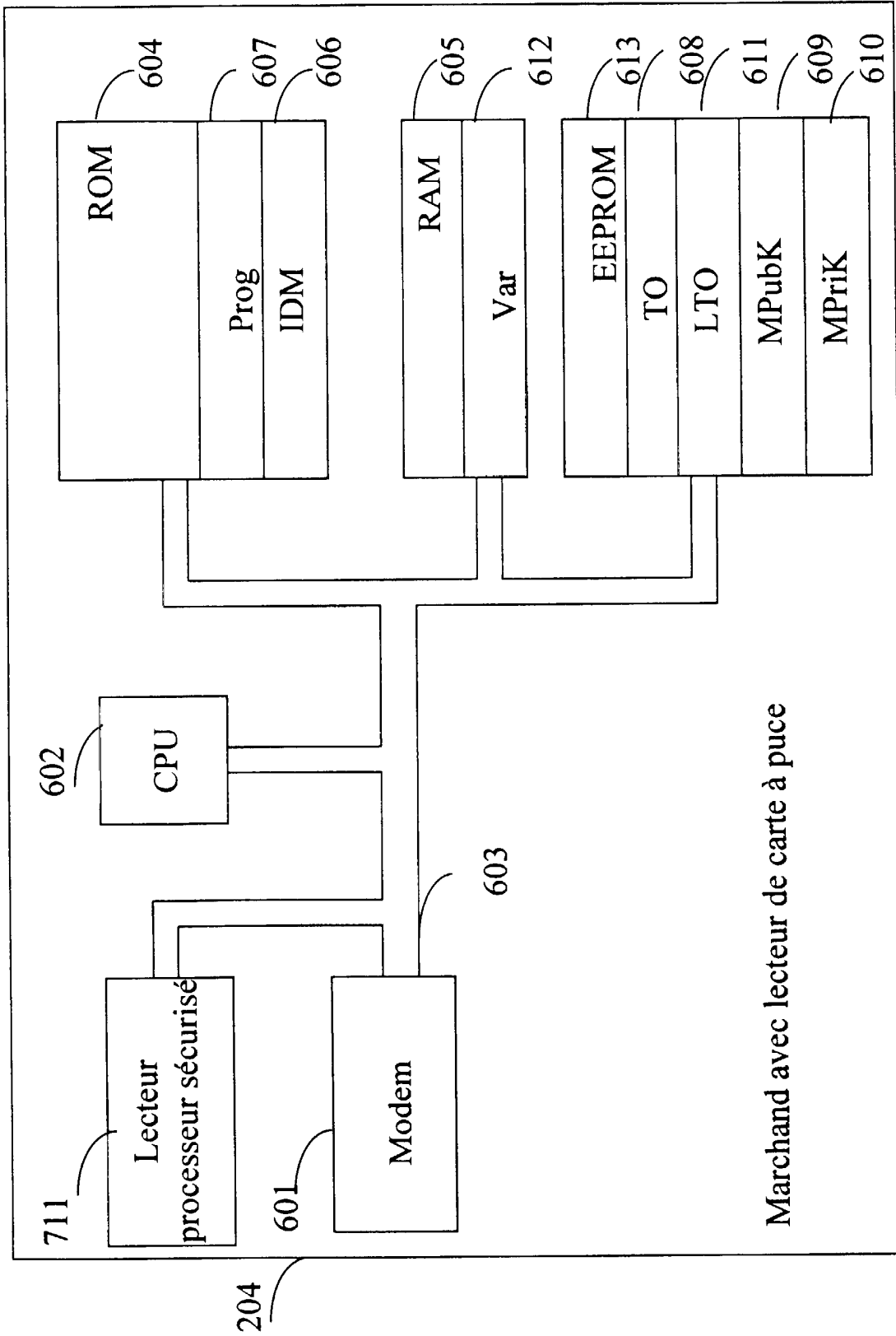


Fig. 7

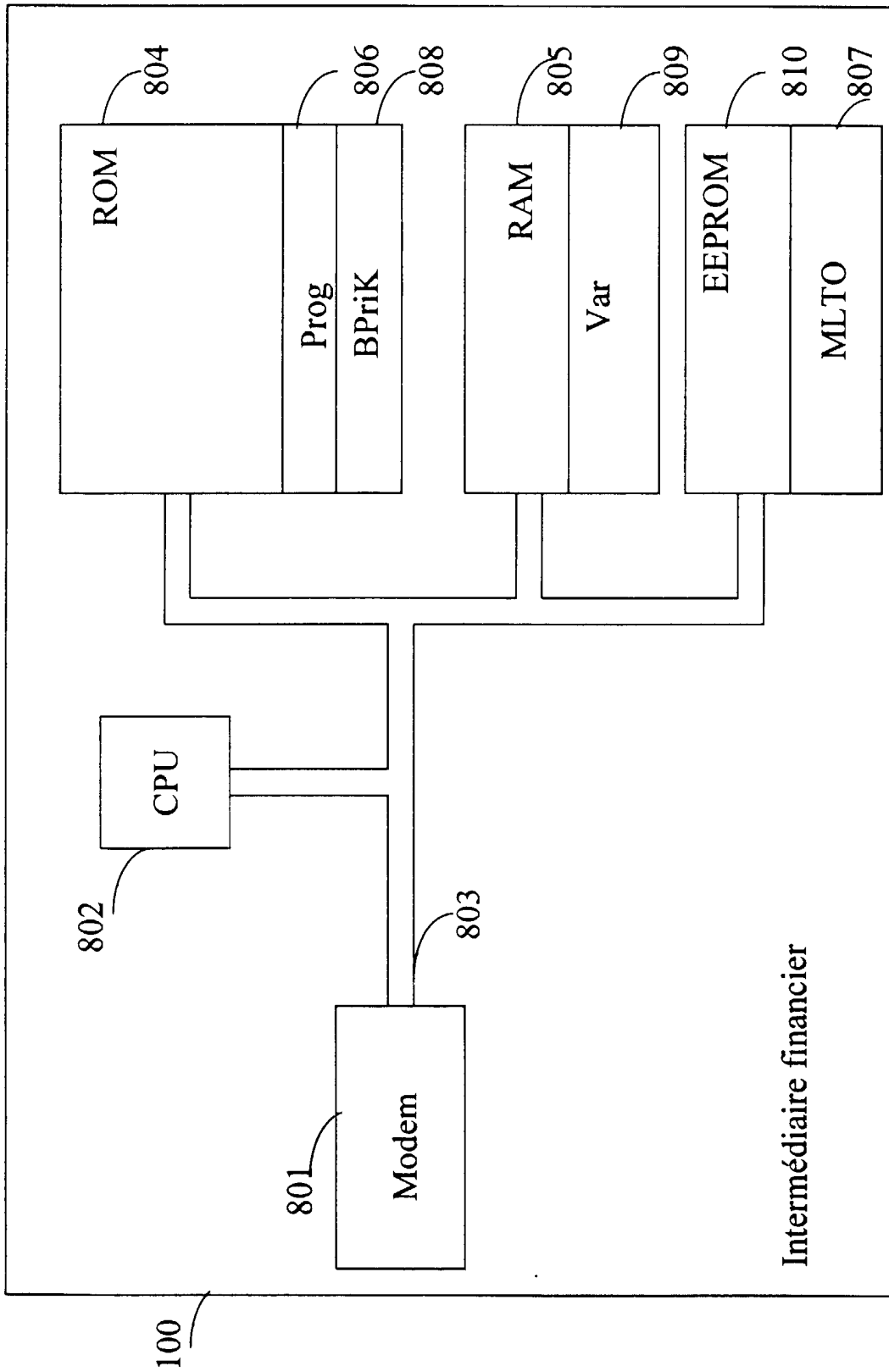


Fig. 8

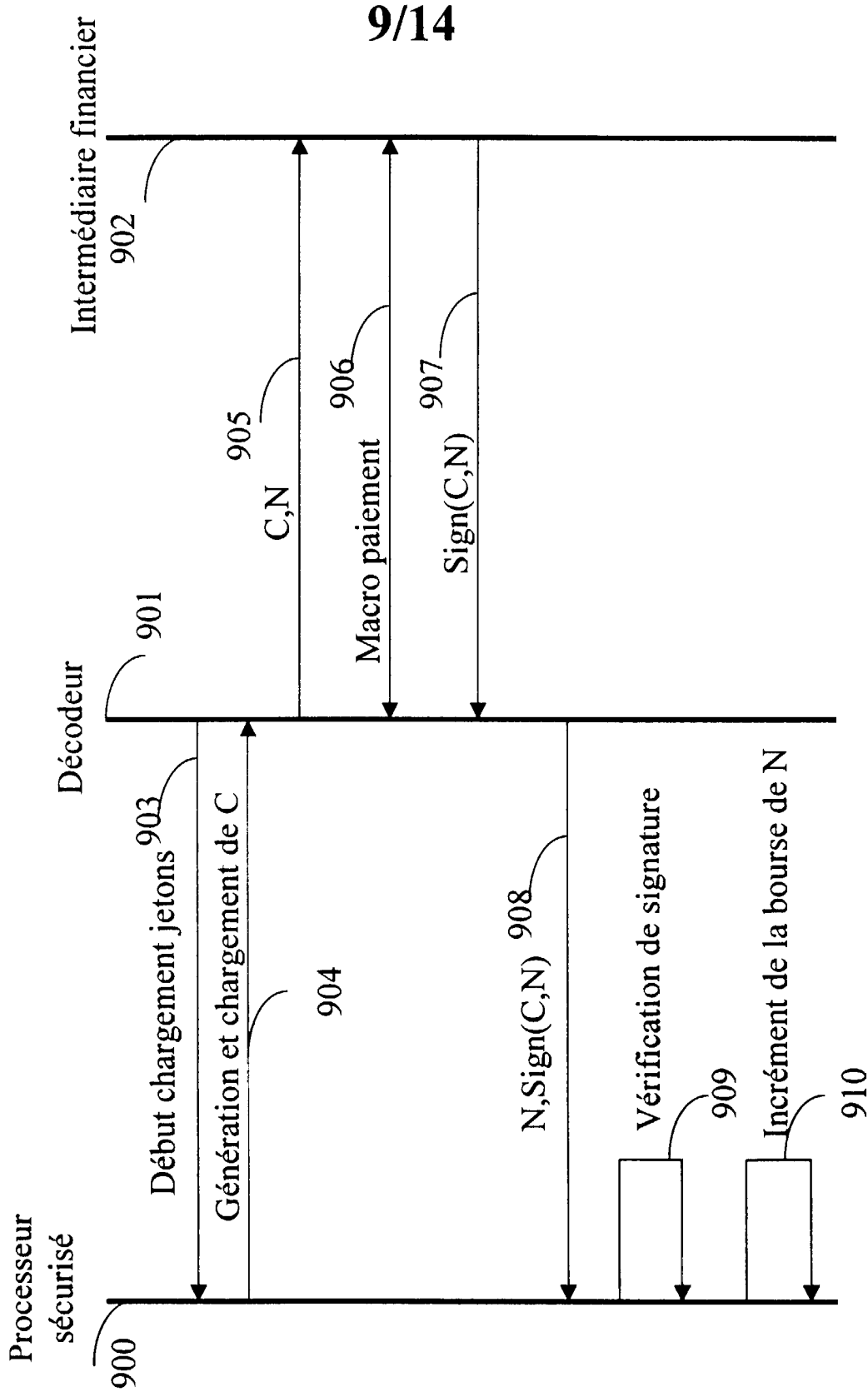


Fig. 9

10/14

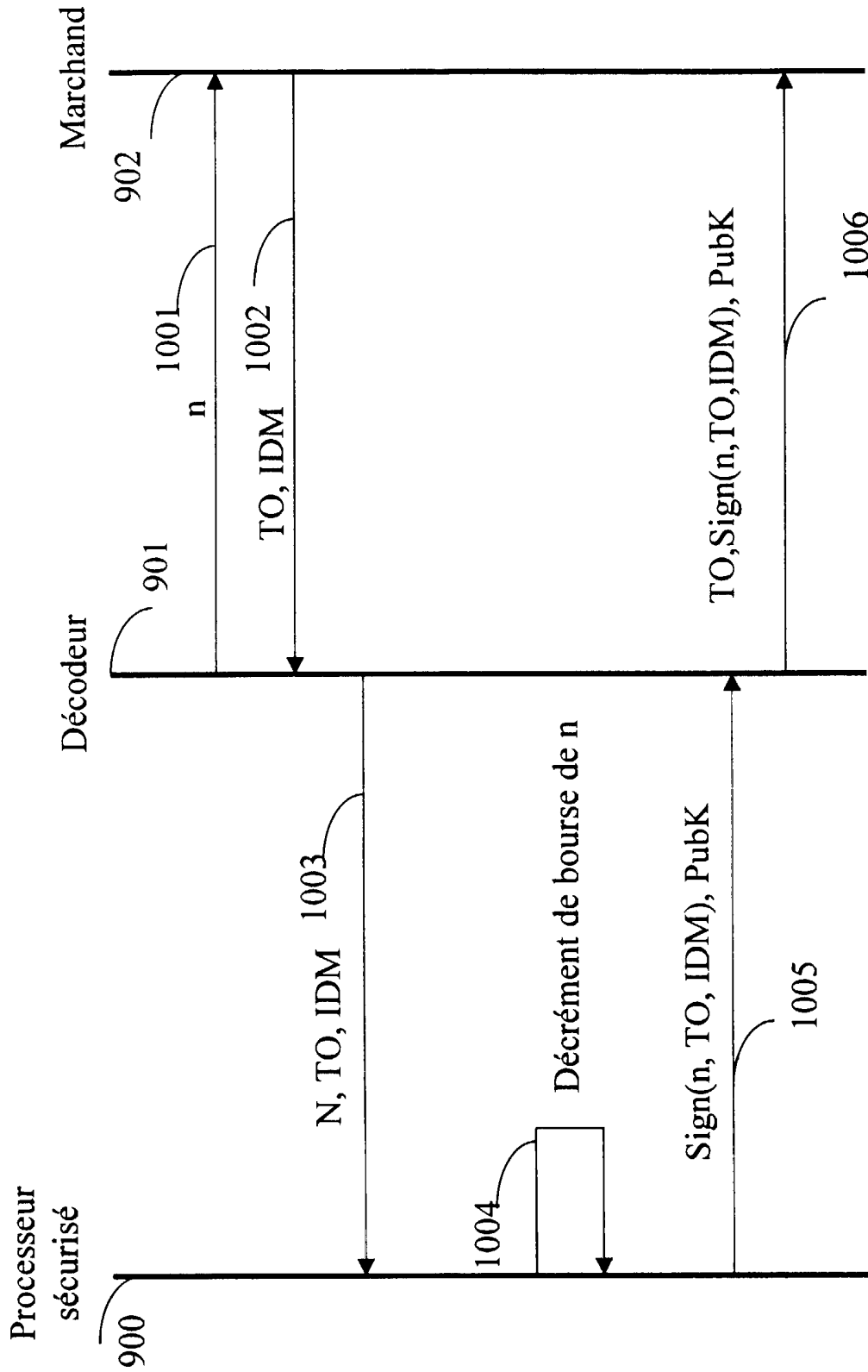


Fig. 10

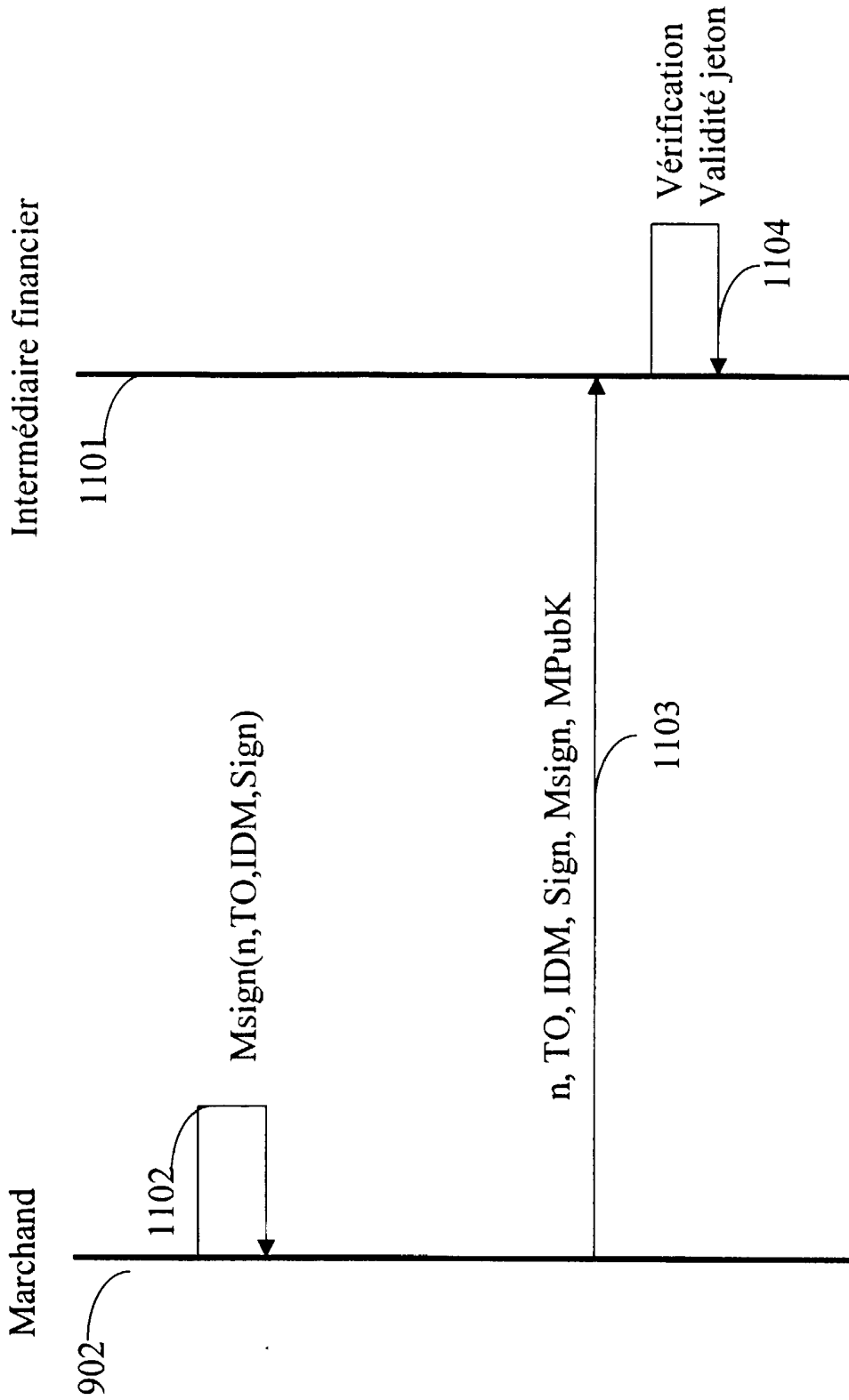
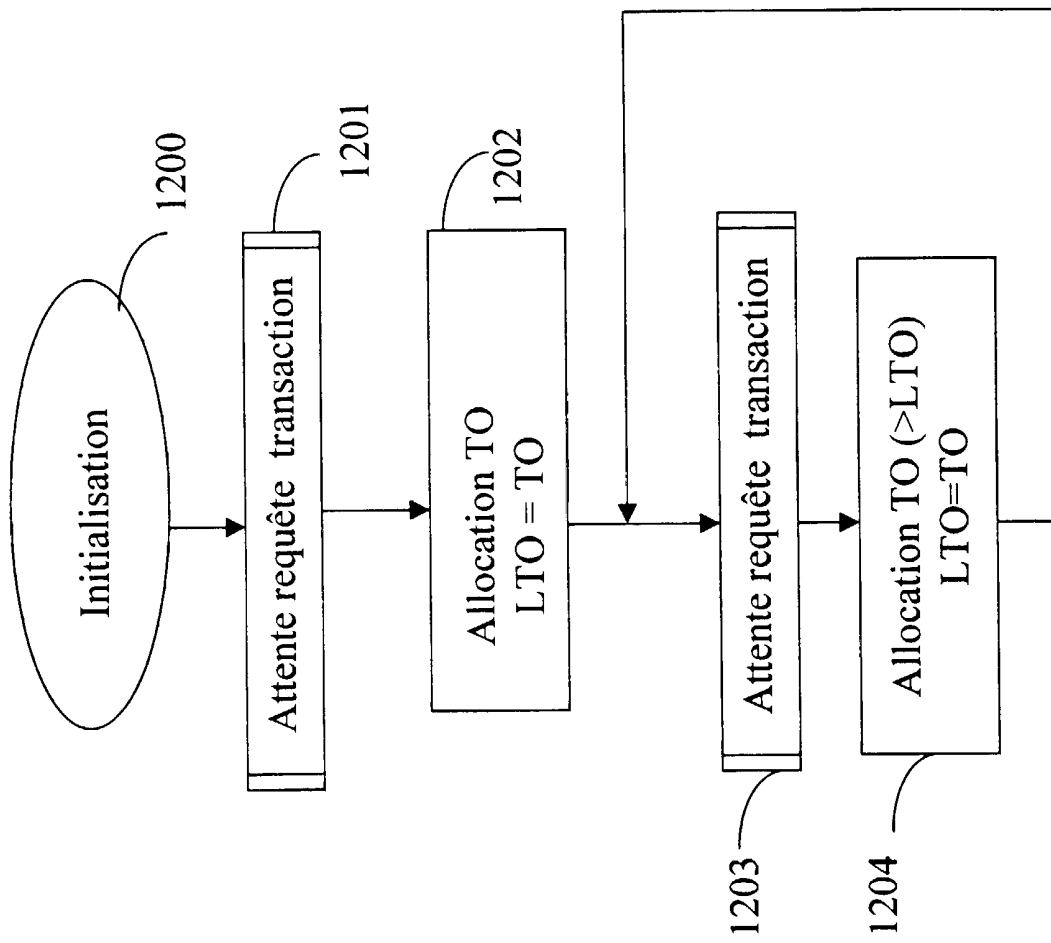


Fig. 11

12/14

**Fig. 12**

13/14

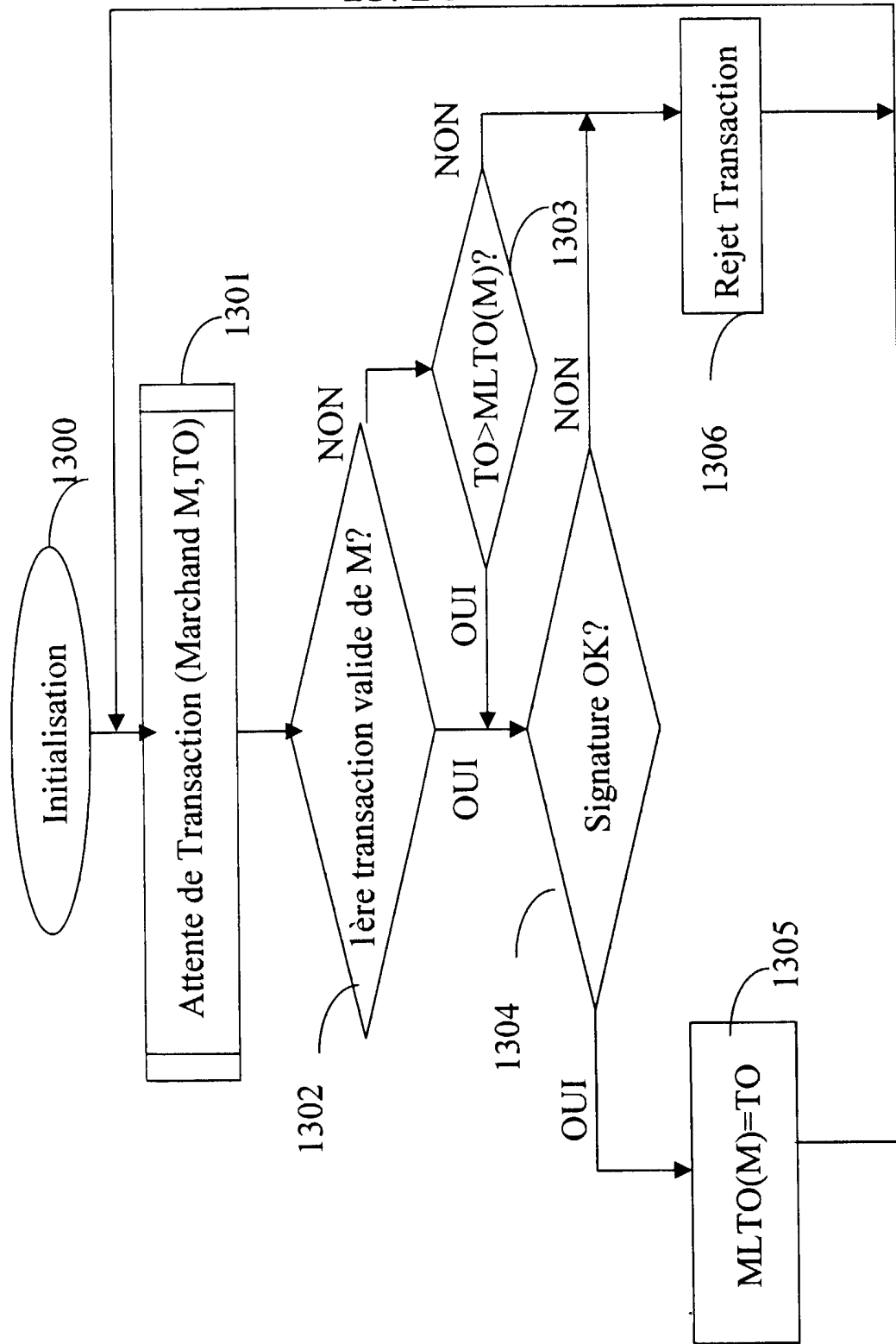


Fig. 13

14/14

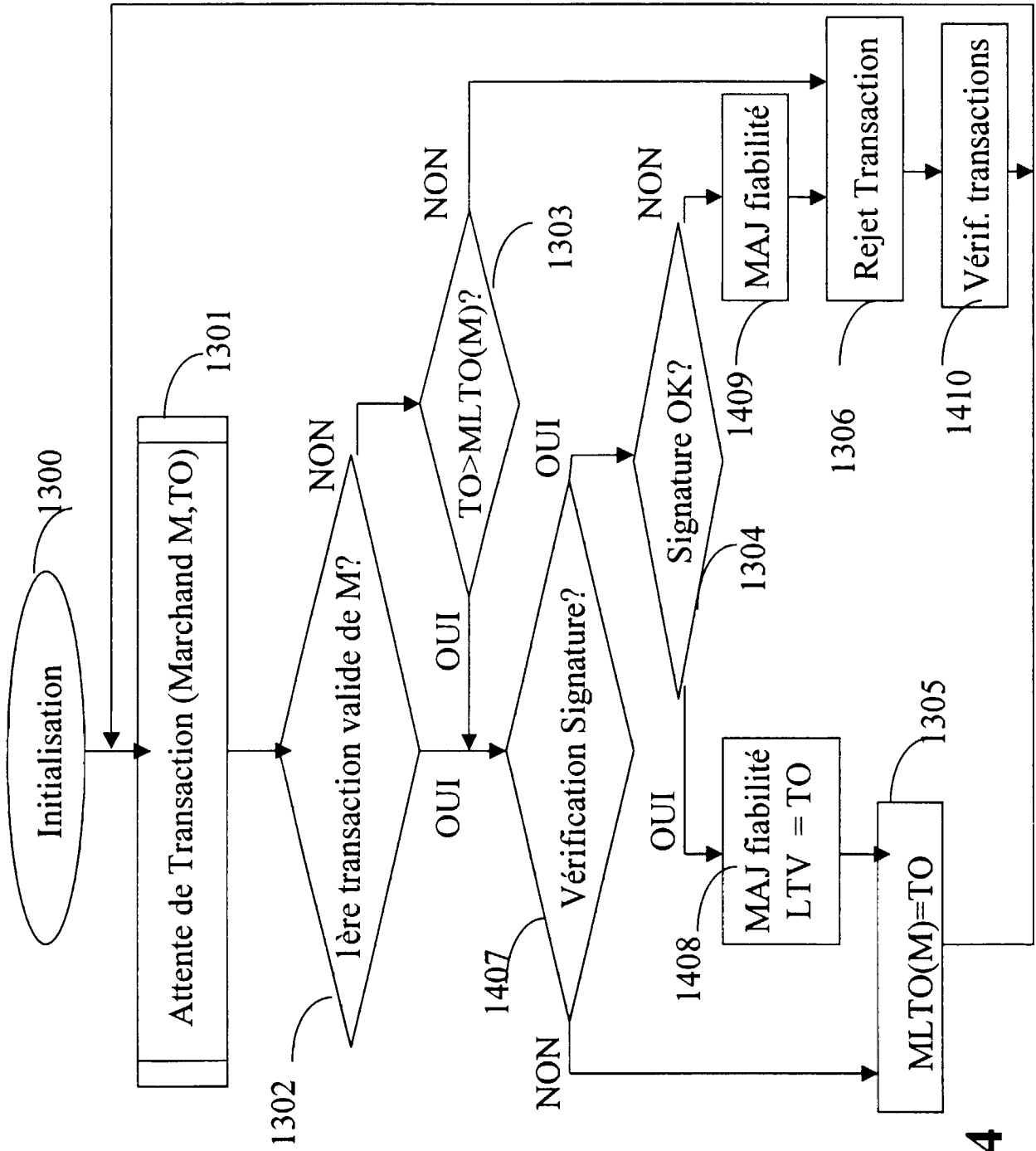


Fig. 14

