(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 742 615**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **96 15323**

(51) Int Cl[6] : H 04 L 9/18, H 04 L 12/28, G 06 F 17/60 //G 06 F 151:00, 157:00

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 13.12.96.

(30) **Priorité** : 14.12.95 US 572425.

(43) **Date de la mise à disposition du public de la demande :** 20.06.97 Bulletin 97/25.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Ce dernier n'a pas été établi à la date de publication de la demande.*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *CYBERCASH, INC.* — US.

(72) **Inventeur(s) :** BOESCH BRIAN PAUL, CROCKER STEPHEN DAVID, EASTLAKE DONALD EGGLESTON, HART JR ALDEN SHERBURNE, LINDENBERG ROBERT A et PAREDES DENISE MARIE.

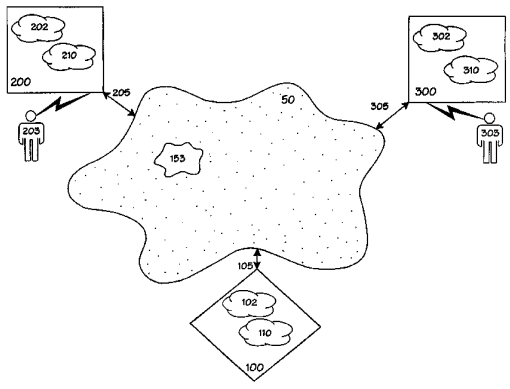
(73) **Titulaire(s) :**

(74) **Mandataire :** NOVAPAT.

(54) PROCEDE ET SYSTEME DE TRANSFERT ELECTRONIQUE DE FONDS PAR DES COMMUNICATIONS DE SECURITE.

(57) On décrit un procédé et un système concernant des communications de sécurité dans un réseau de communication. L'invention utilise des sessions ayant une durée limitée pour permettre aux tiers de communiquer en sécurité dans le réseau. La session d'un tiers est indépendante de celle d'un autre tiers. Les sessions sont liées à un serveur (105) qui confirme qu'elles sont valables.

Dans un mode de réalisation préféré, les communications de sécurité ont lieu dans un système de transfert électronique. Dans ce système, un client (203) et un commerçant (303) peuvent effectuer une transaction dans laquelle le client peut acheter un produit chez le commerçant et le payer en utilisant des fonds électroniques.



FR 2 742 615 - A1

La présente invention concerne un procédé et un dispositif de transfert électronique.

Un chiffrement par code public avec des tailles élevées du code (par exemple système dit RSA) est généralement nécessaire pour créer des niveaux de sécurité acceptables pour le traitement des messages sur un réseau sans sécurité, tel que le réseau Internet. La présente invention concerne un système et un procédé pour augmenter l'efficacité d'un traitement des messages de sécurité dans de tels réseaux qui sont sans sécurité. Plus spécialement, la présente invention est relative à un système et à un procédé pour réduire le niveau du chiffrement nécessaire dans un réseau pour les échanges de messages. D'une manière encore plus spécifique, la présente invention concerne le traitement de transactions électroniques de fonds d'une manière sûre tout en réduisant sensiblement les besoins en calcul pour le chiffrement.

Dans la technique antérieure, on a décrit divers procédés pour augmenter la sécurité des communications dans des réseaux sans sécurité, tels que le réseau Internet. Un réseau sans sécurité ne protège pas les messages contre l'observation, l'interception et la manipulation. D'autre part, les réseaux de sécurité offrent divers moyens pour réduire l'opportunité de l'observation, de l'interception et/ou de la manipulation des messages.

Par exemple, les agencements de sécurité des messages par canal (tels que les protocoles dits HTTP de sécurité ("S-HTTP") et le protocole Secure Socket Layer (SSL) ont pour objet de créer la confiance entre les deux tiers qui communiquent, lesquels sont ceux disant qui ils sont et que leurs communications sont privées. Le protocole SSL utilise des certificats signés numériquement pour fournir authentification et sécurité par un chiffrement lourd de chaque message. Le protocole S-HTTP table sur des messages signés numériquement ayant

un code de chiffrement lourd pour assurer la sécurité et l'authentification.

On a proposé un certain nombre de protocoles multi-parties pour les transactions de crédit, les plus connus étant les Secure Transport Technology (STTP), Internet Keyed Payments (IKP) et Secure Electronic Payment Protocol (SEPP) (Technologie de Transport de Sécurité, Paiements codés Internet et Protocole de Paiement Electronique de Sécurité). Toutes ces approches sont construites autour d'une autorité émettant des lettres de créance et imposent que les commerçants et les clients soient authentifiés par cette autorité, laquelle a été à son tour identifiée par une autorité supérieure. Dans le système STT, les commerçants et les clients ont chacun deux jeux de codes RSA, l'un devant être utilisé pour signer des messages et l'autre pour le chiffrement et le déchiffrement de codes symétriques. Ainsi, dans ce système, chaque partie a besoin de deux certificats (un pour chaque code). Un commerçant aura une paire de lettres de crédit pour chaque carte de crédit qu'il accepte. Les systèmes SEPP et IKP utilisent différemment le chiffrement RSA; mais, d'une manière identique au STT, utilisent de multiples signatures de code public et des chiffrements par transaction.

Un autre système a été décrit sous le nom "NetBill". Alors que la solution NetBill dépend moins du chiffrement par code public que les autres, elle nécessite encore des signatures par code public dans une transaction.

Une autre approche est celle du DigiCash. Dans le modèle DigiCash, l'utilisateur crée un nombre aléatoire, qui agit comme un nombre sériel pour une pièce numérique. Comme les autres systèmes proposés, le DigiCash atteint son objectif principal d'un système de paiement comptant sûr, anonyme, en exigeant une grande confiance sur l'exponentiation modulaire (qui est la base pour d'autres techniques à code public telles que le chiffrement RSA). Cela nécessite aussi une banque ou

un tiers pour créer des jetons qui ont une valeur intrinsèque. La façon avec laquelle un tel système sera traité en matière de transaction bancaire, de taxe et de lois sur les devises aux Etats-Unis et dans d'autres juridictions est incertaine.

D'autres systèmes, tels que le Mondex, mettent en oeuvre la sécurité par l'utilisation d'un matériel connecté à l'ordinateur de l'utilisateur. Pour les transactions sur Internet, un lecteur de carte de propriétaire doit être ajouté aux ordinateurs de tous les clients et les commerçants qui utiliseront une carte particulière.

La confiance sur le chiffrement, en particulier sur le chiffrement par code public, qu'il soit basé ou non sur un logiciel ou un matériel a un certain coût : plus l'utilisation du chiffrement est grande, plus l'effort de traitement nécessaire au décryptage des messages est élevé. Dans le cas où les coûts du traitement des messages sont importants, par exemple, dans les transactions commerciales de paiement sur réseau, les coûts des processeurs et du matériel deviennent un obstacle important à l'utilisation de réseaux tels que l'Internet pour des communications de sécurité.

La technique courante ne peut obtenir qu'une sécurité acceptable avec le coût élevé concomitant du temps du processeur, du matériel supplémentaire, ou des deux. Ce qui est nécessaire pour encourager le développement de réseaux sans sécurité tels que l'Internet à des fins commerciales est un système à base de logiciel qui offre des coûts de traitement réduits des messages chiffrés tout en maintenant un niveau acceptable de la sécurité pour les communications qui sont transmises.

En conséquence, la présente invention a pour objet un système et un procédé pour des transactions très efficaces, économiques et sûres sur le réseau Internet, ou sur d'autres réseaux sans sécurité. Elle

fournit la base pour la mise en oeuvre d'un paiement d'une valeur relativement petite, de sécurité (dont les petits paiements comptants) pour des produits par le réseau Internet ou par d'autres réseaux sans sécurité.

Selon la présente invention, on a découvert un procédé pour des communications sûres dans un système de communication. Le système de communication comprend un premier dispositif à un premier emplacement d'un tiers, un second dispositif à l'emplacement d'un second tiers, et un serveur en communication avec eux. Le procédé comprend la création d'une première session associée au premier tiers, où celle-ci a des premiers paramètres d'utilisation pour limiter la durée d'utilisation de ladite première session et un premier ensemble de données. Les premiers paramètres d'utilisation et ledit premier ensemble de données peuvent être identifiés par le serveur. Le procédé comprend aussi la création d'une seconde session associée au second tiers. La seconde session a des seconds paramètres d'utilisation pour limiter la durée d'utilisation de cette seconde session et un second ensemble de données. Les seconds paramètres d'utilisation et ledit second ensemble de données sont identifiables par le serveur. Le procédé comprend en outre le fait de lier une partie de la première session à une partie de la seconde session dans le système de communication. La partie de la première session comprend ledit premier ensemble de données et lesdits premiers paramètres d'utilisation et la partie de la seconde session comprend le second ensemble de données et les seconds paramètres d'utilisation. Le procédé comporte en outre la vérification des premier et second tiers sur la base d'au moins des portions des premier et second ensembles de données par le serveur, et la détermination du fait que les première et seconde sessions peuvent être ou non utilisées sur la base des premier et second paramètres d'utilisation par le serveur. Lorsque le serveur vérifie les premier et second tiers et procède à

la détermination du fait que les première et seconde sessions peuvent être utilisées, les premier et second tiers sont assurés de communiquer avec sécurité dans le système de communication.

Un autre aspect de la présente invention a pour objet un procédé pour communiquer avec sûreté dans le système de communication. Le système de communication comporte un dispositif à l'emplacement de l'utilisateur et un serveur en communication avec lui, et le procédé comporte la transmission d'une demande émanant du dispositif vers le serveur pour créer une session ayant des paramètres d'utilisation associés à elle, le chiffrement d'un premier code avec un second code par le serveur, et la transmission du premier code chiffré et des paramètres d'utilisation associés à la première session entre le serveur et le dispositif. Le procédé comprend aussi la réception du premier code chiffré et des paramètres d'utilisation par le dispositif et le déchiffrage du premier code chiffré de façon que le dispositif puisse communiquer avec sûreté dans le système de communication en employant le premier code déchiffré en conformité avec les paramètres d'utilisation.

La présente invention sera bien comprise lors de la description suivante faite en liaison avec les dessins ci-joints dans lesquels :

La figure 1 représente l'architecture générale de la présente invention.

La figure 2 représente les opérations générales de la présente invention.

La figure 3A représente plus particulièrement les opérations indiquées en figure 2.

La figure 3B représente la circulation des messages dans la présente invention.

La figure 4A représente la structure de la base de données de l'ordinateur 100 du serveur.

La figure 4B représente un état civil 120.1 de client d'une structure 120 de données d'état civil de serveur.

La figure 4C décrit les champs de données 120G d'un conteneur d'espèces de la figure 4B.

La figure 4D décrit les champs de données 120H du lien à un instrument financier de la figure 4B.

La figure 4E décrit un état civil 120.2 du commerçant de la structure 120 de données d'état civil du serveur.

La figure 4F décrit les champs des données 120GG du conteneur d'espèces de la figure 4E.

La figure 4G décrit les champs des données 120HH du lien à un instrument financier de la figure 4E.

La figure 4H décrit l'enregistrement 130.1 de la session-client de la structure de données de la session-serveur.

La figure 4I décrit les champs des données de transaction 130N de la figure 4H.

La figure 4J décrit l'enregistrement 130.2 de l'enregistrement de la session du commerçant de la structure des données de la session du serveur.

La figure 4K décrit les champs des données de transaction 130NN de la figure 4J.

La figure 4L décrit un enregistrement 140.1 de la structure 140 des données du journal des messages.

La figure 5A décrit la structure de la base de données de l'ordinateur 200 du client.

La figure 5B décrit l'enregistrement 215.1 de la structure 215 des données d'application du client.

La figure 5C décrit l'enregistrement 220.1 de la structure 220 des données d'état civil du client.

La figure 5D décrit l'enregistrement 230.1 de la structure 230 des données du lien à un instrument financier du client.

La figure 5E décrit l'enregistrement 240.1 de la structure 240 des données de session active du client.

La figure 5F décrit la structure 250 des données du journal en attente du client.

La figure 5G décrit l'enregistrement 251 des informations d'état civil pour une inscription/mise à jour de la structure 250 des données de transaction en attente du client.

La figure 5H décrit l'enregistrement 252 de liaison/mise à jour en attente du lien à un instrument finàncier de la structure 250 des données de transaction en attente du client.

La figure 5I décrit l'enregistrement 253 des paiements en espèces en attente de la structure 250 des données de transaction en attente du client.

La figure 5J décrit l'enregistrement 254 de chargement/déchargement des fonds en attente de la structure 250 des données de transaction en attente du client.

La figure 5K décrit l'enregistrement 255 de l'ouverture d'une session en attente de la structure 250 des données de transaction en attente du client.

La figure 5L décrit l'enregistrement 256 de la clôture d'une session en attente de la structure 250 des données de transaction en attente du client.

La figure 5M décrit la structure 260 des données du journal du client.

La figure 5N décrit l'enregistrement 261 de la réponse de l'instrument à une inscription/mise à jour de la structure 260 des données du journal du client.

La figure 5O décrit l'enregistrement 262 de la réponse de la liaison/mise à jour de la structure 260 des données d'enregistrement du client.

La figure 5P décrit l'enregistrement 263 de la réponse au paiement comptant de la structure 260 des données du journal du client.

La figure 5Q décrit l'enregistrement 264 de la réponse au chargement/déchargement des fonds de la structure 260 des données du journal du client.

La figure 5R décrit l'enregistrement 265 de la réponse à l'ouverture d'une session de la structure 260 des données du journal du client.

La figure 5S décrit l'enregistrement 266 des demandes de paiement de la structure 260 des données du journal du client.

La figure 5T décrit l'enregistrement 267 de la réponse à la clôture d'une session de la structure 260 des données du journal du client.

La figure 5U décrit un enregistrement 280.1 de la structure 280 des données du conteneur d'espèces du client.

La figure 6A décrit la structure de la base de données de l'ordinateur du commerçant.

La figure 6B décrit un enregistrement de la structure des données d'application du commerçant de la base de données de l'ordinateur du commerçant.

La figure 6C décrit un enregistrement de la structure des données d'état civil du commerçant de la base de données de l'ordinateur du commerçant.

La figure 6D décrit un enregistrement de la structure des données du lien à un instrument financier du commerçant de la base de données de l'ordinateur du commerçant.

La figure 6E décrit un enregistrement de la structure des données de session du commerçant de la base de données de l'ordinateur du commerçant.

La figure 6F décrit un enregistrement de la structure des données du conteneur d'espèces du commerçant de la base de données de l'ordinateur du commerçant.

La figure 7A décrit un enregistrement de la structure des données de montant du commerçant de la base de données de l'ordinateur du commerçant.

La figure 7B décrit un enregistrement de la structure des données de la session de ventes du commerçant de la base de données de l'ordinateur du commerçant.

La figure 7C décrit un enregistrement de la structure des données du journal des espèces du commerçant de la base de données de l'ordinateur du commerçant.

La figure 7D décrit le format d'un message échantillon.

La figure 8 est un organigramme du mode opératoire d'inscription 401.

La figure 9 est un organigramme du mode opératoire 800 d'assemblage de message.

Les figures 10A et 10B décrivent le format d'un message d'inscription R1.

Les figures 11A et 11B représentent un organigramme du mode opératoire 900 de dévoilement d'un message de serveur.

La figure 12 est un organigramme d'un mode opératoire 1000 d'assemblage de message du serveur.

Les figures 13A et 13B décrivent le format d'un message d'inscription R2.

La figure 14 est un organigramme représentant le mode opératoire 1100 du dévoilement d'un message de client.

La figure 15 est un organigramme représentant l'opération 403 de lien à un instrument financier.

Les figures 16A et 16B décrivent le format du message de lien BI1.

Les figures 17A et 16B décrivent le format d'un message de lien BI4.

La figure 18 est un organigramme représentant l'opération 405 de chargement/déchargement de fonds.

Les figures 19A et 19B décrivent le format d'un message de chargement/déchargement LU1.

Les figures 20A et 20B décrivent le format d'un message de chargement/déchargement LU2.

La figure 21 est un organigramme représentant l'opération 407 d'ouverture de session.

Les figures 22A et 22B décrivent le format d'un message d'ouverture de session OS1.

Les figures 23A et 23B décrivent le format d'un message d'ouverture de session OS2.

Les figures 24A, 24B et 24C décrivent un organigramme représentant une opération de transaction/ paiement 409.

La figure 25 décrit le format d'un message de demande de paiement PR1.

La figure 26 est un organigramme du mode opératoire 3300 de dévoilement d'un message.

La figure 27 est un organigramme représentant le mode opératoire d'assemblage d'un message CA12.

La figure 28 décrit le format d'un message de paiement comptant CA1.

La figure 29 est un organigramme du mode opératoire de génération code CA-DES.

La figure 30 est un organigramme décrivant le mode opératoire de dévoilement de message CA1.

Les figures 31A, 31B et 31C décrivent le format d'un message CA2.

Les figures 32A et 32B sont un organigramme du mode opératoire 1660 de dévoilement d'un message du serveur.

La figure 33 est un organigramme du mode opératoire 3400 d'assemblage d'un message du serveur.

Les figures 34A, 34B et 34C décrivent le format d'un message CA3.

La figure 35 est un organigramme du mode opératoire CA34 de dévoilement d'un message.

La figure 36 est un organigramme du mode opératoire 3100 d'assemblage d'un message.

Les figures 37A et 37B décrivent le format d'un message CA4.

La figure 38 est un organigramme du mode opératoire de clôture de session 411.

Les figures 39A et 39B décrivent le format d'un message CS1.

Les figures 40A et 40B décrivent le format d'un message CS2.

On se reportera maintenant aux figures 1-40 pour avoir une description détaillée des modes de réalisation préférés de la présente invention. Les figures et la description les accompagnant ne sont pas destinées à limiter le domaine de la présente invention.

I. Information et circulation de l'information.

On décrit dans ses grandes lignes la présente invention en figure 1. La figure 1 représente trois entités : un ordinateur de serveur 100, un ordinateur de client 200 et un ordinateur de commerçant 300, connectés les uns aux autres via le réseau Internet 50. Les connexions sont identifiées par des lignes 105, 205 et 305, respectivement.

L'ordinateur 200 du client représente l'ordinateur d'un utilisateur individuel client 203, qui veut acheter un produit par l'intermédiaire du réseau Internet 50. (Un "produit" comprend des marchandises, des services, des informations, des données, etc.). L'ordinateur 200 du client comprend une base de données de client 202 et un logiciel d'application de client 210. L'ordinateur 300 du commerçant représente l'ordinateur d'un utilisateur individuel, commerçant 303, qui fournit le produit à l'utilisateur-client 203 par l'intermédiaire du réseau Internet 50. L'ordinateur 300 du commerçant comprend une base de données de commerçant 302 et un logiciel d'application de commerçant 310. Une information relative à l'utilisateur-commerçant 303 est stockée dans la base de données 302 du commerçant. Le logiciel d'application du commerçant 310 exécute les opérations de la présente invention.

Alors qu'on donne la description détaillée suivante pour un seul utilisateur-client 203 et un seul utilisateur-commerçant 303, on remarquera que la présente invention envisage les communications et transactions entre des utilisateurs clients uniques et multiples 203 et des utilisateurs commerçants uniques et multiples 303.

L'ordinateur 100 du serveur communique avec sécurité - comme on le décrira ultérieurement en détail - avec l'ordinateur 200 du client et l'ordinateur 300 du commerçant par le réseau Internet 50 afin d'effectuer les transactions entre l'utilisateur client 203 et l'utilisateur commerçant 303. L'ordinateur 100 du serveur comprend une base de données de serveur 102 et un logiciel de serveur 110. Une information relative à l'ordinateur 100 du serveur, à l'utilisateur client 203 et à l'utilisateur commerçant 303 est stockée dans la base de données 102 du serveur. Le logiciel 110 du serveur exécute les opérations de la présente invention.

La communication entre l'ordinateur 100 du serveur, l'ordinateur 200 du client et l'ordinateur 300 du commerçant est de préférence exécutée par le protocole de transport hypertext ("HTTP") par les services World Wide Web("WWW") fournis sur le réseau Internet 50. Naturellement, on peut utiliser ou désirer d'autres protocoles et réseaux.

La figure 2 décrit les opérations générales exécutées par la présente invention. Les opérations commencent à l'étape 0.

Tout d'abord, les opérations d'établissement sont exécutées à l'étape 1. Dans les opérations d'établissement, l'utilisateur client 203 et l'utilisateur commerçant 303 (collectivement les "clients du système") sont configurés dans la base de données 102 de l'ordinateur 100 du serveur. De cette manière, les clients du système peuvent être reconnus et communiquer avec l'ordinateur 100 du serveur. La base de

données 202 du client et la base de données 302 du commerçant sont également configurées à l'étape 1.

Une opération d'ouverture de session est exécutée à l'étape 2. En général, une session est une opportunité (ou fenêtre) dans laquelle l'utilisateur client 203 peut acheter un produit auprès de l'utilisateur commerçant 303 par l'intermédiaire du réseau Internet 50 ou dans laquelle l'utilisateur 303 peut fournir un produit à l'utilisateur client 203 par le réseau Internet 50. L'utilisateur client 203 et l'utilisateur commerçant 303 ont leurs propres sessions indépendantes. Les sessions sont d'une durée limitée. Cette durée est dictée par des paramètres. Ces paramètres sont de préférence établis par l'utilisateur client 203 et l'utilisateur commerçant 303. En variante, l'ordinateur 100 du serveur peut établir de tels paramètres.

Une opération de transaction/paiement est exécutée à l'étape 3. Dans cette étape, l'utilisateur client 203 et l'utilisateur commerçant 303 se mettent d'accord sur un produit devant être fourni à un prix agréé. L'utilisateur client 203 paie le produit par paiement électronique. Le paiement électronique est une représentation de fonds (espèces réelles, crédit, etc.) utilisée dans la présente invention. Le paiement électronique est reçu par l'utilisateur commerçant 303 qui peut fournir le produit acheté à l'utilisateur client 203. L'utilisateur client 203 peut faire des affaires avec de multiples utilisateurs commerçants 303 lors d'une session. L'utilisateur client 203 et l'utilisateur commerçant 303 sont seuls à même de faire des transactions commerciales pendant la durée des sessions telles que celles créées à l'étape 2.

Une opération de clôture de session peut être incluse dans la présente invention à l'étape 4. Cette étape termine la session créée à l'étape 2.

Les opérations exécutées par la présente invention se terminent à l'étape 5.

En liaison avec la figure 3A, les opérations décrites ci-dessus dans les étapes 1 à 4 de la figure 2 sont maintenant plus particulièrement décrites. Tout d'abord, les opérations d'établissement exécutées à l'étape 1 comprennent une opération de téléchargement et d'installation 400, une opération d'inscription 401, une opération de lien à un instrument financier 403 et une opération de chargement/déchargement de fonds 405.

Pendant l'opération 400 de téléchargement et d'installation, l'utilisateur client 203 et l'utilisateur commerçant 303 téléchargent chacun et installent une copie du logiciel d'application client 153 (figure 1) qui réside de préférence sur le réseau Internet 50. Dans l'ordinateur 200 du client et dans l'ordinateur 300 du commerçant, la copie du logiciel d'application client 153 réside sous forme de logiciel d'application client 210 et de logiciel d'application commerçant 310, respectivement. (Le logiciel d'application commerçant 310 comprend un autre logiciel pour permettre à l'ordinateur 300 du commerçant d'exécuter les fonctions décrites ci-dessous). En utilisant des techniques bien connues, le logiciel d'application client 210 et le logiciel d'application commerçant 310 sont liés au dispositif de consultation web de l'ordinateur 200 du client et de l'ordinateur 300 du commerçant, respectivement, et sont accédés par l'intermédiaire de ce dispositif selon nécessité.

Ensuite, à une opération d'inscription 401, l'utilisateur client 203 et l'utilisateur commerçant 303 s'inscrivent dans l'ordinateur 100 du serveur. Plus précisément, un "état civil" pour l'utilisateur client 203 et les utilisateurs commerçants 303 est créé dans la base de données 102 de l'ordinateur 100 du serveur. Un "état civil" est défini ici par un ensemble de données concernant un client spécifique. Par conséquent, grâce à ce procédé d'inscription, chaque utilisateur client 203 et utilisateur commerçant 303 qui a été inscrit dans l'ordinateur 100 du serveur a son propre état civil dans

l'ordinateur 100. (On décrira ultérieurement les détails des états civils). Le droit d'un état civil à exécuter certaines opérations (par exemple, charger des fonds, décharger des fonds, soumettre certains messages à l'ordinateur 100 du serveur) peut être validé ou invalidé sur la base d'un message ou d'un service.

Pendant l'opération 403 de lien à l'instrument financier de la figure 3A, un donneur d'ordre (un utilisateur client 203 ou un utilisateur commerçant 303) communique une information à l'ordinateur 100 du serveur qui l'utilise pour établir le fait que le donneur d'ordres peut utiliser un instrument financier. Les instruments financiers peuvent comprendre des cartes de crédit, des cartes de débit, des comptes de dépôt à la demande ("CDA") ou autres instruments financiers. L'émetteur de l'instrument qui est lié ou une garantie d'un tiers établit les critères qu'il considère comme nécessaires pour déterminer si le donneur d'ordres peut utiliser l'instrument. Par exemple, une banque émettant une carte de crédit peut trouver qu'il est suffisant que le donneur d'ordres fournisse un code postal à cinq chiffres et le nom de jeune fille de sa mère dans le but d'utiliser la carte de crédit. Une liste de ces critères peut, par exemple, être fournie à l'ordinateur 100 du serveur, auquel cas cet ordinateur 100 peut communiquer avec le donneur d'ordres pour établir le fait que ce donneur d'ordres satisfait ou non ces critères de sorte qu'il peut utiliser l'instrument financier.

Dès que le donneur d'ordres établit le fait qu'il peut utiliser l'instrument par cette opération, l'instrument est "lié" ou associé à l'état civil du donneur d'ordres qui est créée pendant l'opération d'inscription 401. Dès que l'instrument est lié, le donneur d'ordres peut utiliser l'instrument pour des transactions comme on le décrira ultérieurement.

On discutera maintenant l'opération 405 de chargement/déchargement de fonds. Pour l'utilisateur

client 203, un "chargement" est l'opération dans laquelle des fonds associés à un instrument lié sont "chargés" (ou transférés) à l'état civil de l'utilisateur client 203. Dans l'état civil de l'utilisateur client 203, les fonds sont représentés comme des espèces électroniques. Pour l'utilisateur client 203, un "déchargement" est l'opération dans laquelle les espèces électroniques sont "déchargées" (ou transférées) de l'état civil de l'utilisateur client 203 à un instrument lié. Pour l'utilisateur commerçant 303, un "déchargement" est l'opération dans laquelle les espèces électroniques sont "déchargées" à partir de l'état civil de l'utilisateur commerçant 303 dans un instrument lié. Pour l'utilisateur commerçant 303, un "chargement" est l'opération dans laquelle les fonds associés à un instrument lié sont "chargés" dans l'état civil de l'utilisateur commerçant 303. Dans l'état civil de l'utilisateur commerçant 303, les fonds sont représentés par des espèces électroniques.

On expliquera davantage l'opération d'ouverture de session pour l'étape 2 de la figure 2 en ce qui concerne l'opération d'ouverture de session 407 de la figure 3A. Lorsque l'utilisateur client 203 crée une session, il peut faire une transaction commerciale par l'Internet 50 avec un ou plusieurs utilisateurs commerçants 303 qui ont créée chacun leurs propres sessions indépendantes. (Naturellement, les utilisateurs commerçants 303 peuvent aussi agir en utilisateurs clients 203 s'ils le désirent).

L'opération de transaction/paiement 409 est ensuite exécutée. Au cours de cette opération, l'utilisateur client 203 et l'utilisateur commerçant 303 peuvent négocier et se mettre d'accord sur les éléments d'une transaction (par exemple un produit particulier et un prix). Alors, l'utilisateur commerçant 303 peut demander que l'utilisateur client 203 paie le prix agréé pour le produit. En réponse à la demande de l'utilisateur commerçant 303, l'utilisateur client 203

peut communiquer avec l'utilisateur commerçant 303 pour indiquer que l'utilisateur client 203 accepte le prix agréé pour le produit. On préfère que l'utilisateur commerçant 303 fasse en sorte que l'information relative à la transaction soit soumise à l'ordinateur 100 du serveur pour validation. Si l'ordinateur 100 valide la transaction, les espèces électroniques sont transférées de l'état civil de l'utilisateur client 203 à l'état civil de l'utilisateur commerçant 303. Dès qu'il y a une notification de la validation, l'utilisateur commerçant 303 peut fournir le produit à l'utilisateur client 203.

Lors de l'opération de clôture de session 411, la session créée pendant l'opération d'ouverture de session 407 peut être terminée. Lorsque l'utilisateur client 203 (ou l'utilisateur commerçant 303) clot la session, l'ordinateur 100 du serveur empêche l'utilisateur client 203 (ou l'utilisateur commerçant 303) de procéder à des transactions par l'Internet 50 avec un autre utilisateur commerçant 303 (ou avec un utilisateur client 203) qui a une session ouverte à moins que l'utilisateur client 203 ait d'autres sessions ouvertes.

En liaison avec la figure 3B qui décrit la circulation des messages de la présente invention, l'opération d'inscription 401 est exécutée par l'ordinateur client 200 en envoyant un message R1 ("Inscription 1") à l'ordinateur 100 du serveur. En réponse au message R1, l'ordinateur 100 envoie un message R2 ("Inscription 2") à l'ordinateur 200 du client. L'information comprise dans ces messages d'inscription sera décrite ultérieurement.

Pendant l'opération 403 de lien à un instrument, l'ordinateur 200 du client envoie un message BI1 ("lien à l'instrument 1") à l'ordinateur 100 du serveur. L'information du message BI1 est utilisée par l'ordinateur 100 du serveur pour confirmer l'autorité du responsable de l'instrument avec l'émetteur de cet instrument ou la garantie d'un tiers. L'opération de

confirmation pourrait être accrue par l'échange de messages (ici, les messages BI2 et BI3) entre l'ordinateur 100 du serveur et l'ordinateur 200 du client. Les messages BI2 et BI3 auraient un format similaire à celui des autres messages qu'on décrit ici. Le contenu du message BI2 peut inclure des demandes pour une information supplémentaire (sollicitée par l'émetteur de l'instrument) ou une clarification de l'information telle qu'elle peut être demandée par l'émetteur de l'instrument ou la garantie du tiers. Par exemple, le message BI2 peut faire en sorte que l'utilisateur client 203 sollicite le nom de jeune fille de la mère de l'utilisateur client 203. Le message BI3 peut contenir la réponse de l'utilisateur client 203.

En réponse au message BI1, l'ordinateur 100 du serveur envoie un message BI4 ("Lien à l'Instrument 4") à l'ordinateur 200 du client. On décrira ultérieurement l'information comprise dans ces messages de lien. Dans la description qui suit, les messages BI1 et BI4 sont les messages opérationnels pour le lien d'un instrument.

Pendant l'opération de chargement/ déchargement de fonds 405, l'ordinateur 200 du client envoie un message LU1 ("Chargement/Déchargement 1") à l'ordinateur 100 du serveur. En réponse au message LU1, l'ordinateur 100 du serveur renvoie un message LU2 ("Chargement/Déchargement 2") à l'ordinateur 200 du client. L'information incluse dans ces messages de chargement/déchargement de fonds sera décrite ultérieurement.

Pendant l'opération 407 d'ouverture de session, l'ordinateur 200 du client envoie un message OS1 ("Ouverture de Session 1") à l'ordinateur 100 du serveur. En réponse au message OS1, l'ordinateur 100 du serveur envoie un message OS2 ("Ouverture de Session 2") à l'ordinateur 200 du client. L'information incluse dans ces messages d'ouverture de session sera décrite ultérieurement.

Pendant l'opération de transaction/paiement 409, l'ordinateur 300 du commerçant envoie un message PR1 ("Demande de Paiement 1") à l'ordinateur 200 du client. En réponse au message PR1, l'ordinateur du client renvoie un message CA1 ("Paiement en espèces 1") à l'ordinateur 300 du commerçant. Après réception du message CA1, l'ordinateur du commerçant envoie un message CA3 ("Paiement en espèces 2") à l'ordinateur 100 du serveur. En réponse au message CA2, l'ordinateur 100 du serveur renvoie un message CA3 ("Paiement en espèces 3") à l'ordinateur 300 du commerçant. En réponse au message CA3, l'ordinateur 200 du commerçant envoie un message CA4 ("Paiement en espèces 4") à l'ordinateur 200 du client. On décrira ultérieurement l'information incluse dans ces messages de transaction/ paiement.

Pendant l'opération facultative de clôture de session 411, l'ordinateur 200 du client envoie un message CS1 ("Clôture de Session 1") à l'ordinateur 100 du serveur. En réponse au message CS1, l'ordinateur 100 du serveur envoie un message CS2 ("Clôture de Session 2") à l'ordinateur 200 du client. On décrira ultérieurement l'information incluse dans ces messages de clôture de session.

On remarquera que la figure 3B décrit des messages R1/R2, BI1/BI4, LU1/LU2, OS1/OS2 et CS1/CS2 passant entre l'ordinateur 200 du client et l'ordinateur 100 du serveur. L'utilisateur commerçant 303 fait en sorte que ces mêmes messages circulent entre l'ordinateur 300 du commerçant et l'ordinateur 100 du serveur. Il s'en suit que l'utilisateur commerçant 303 exécute l'opération 401 d'inscription, l'opération 403 de lien à un instrument, l'opération 405 de chargement/ déchargement de fonds, l'opération 407 d'ouverture de session et l'opération 411 de clôture de session de la même façon que l'utilisateur client 203, sauf indication contraire. Dans le cas de l'utilisateur commerçant 303, la donnée associée à ces opérations est manipulée en ce

qui concerne la base de données du commerçant et les structures des données du commerçant incluses dans l'ordinateur 100 du serveur.

On décrira maintenant les bases de données et les structures des données qu'on utilise dans les modes de réalisation préférés de la présente invention.

II. Bases de données.

En liaison avec la figure 1, l'ordinateur 100 du serveur, l'ordinateur 200 du client, et l'ordinateur 300 du commerçant comprennent des bases de données 102, 202 et 302, respectivement. Alors que la description suivante des bases de données 102, 202 et 302 concernent des structures et des formats de données spécifiques, l'homme de l'art remarquera facilement que de tels structures et formats ne sont pas déterminants et ne sont pas considérés comme faisant partie de la présente invention. Par conséquent, toute modification apportée aux structures et formats des données entre dans le domaine des revendications annexées.

On préfère que des valeurs soient stockées dans les bases de données 202 et 302 lorsqu'un message de réponse est reçu par l'ordinateur 200 du client et l'ordinateur 300 du commerçant, respectivement. Cependant, pour améliorer la clarté, les valeurs sont décrites comme étant stockées avant la réception d'un tel message de réponse.

A. Base de données 102 du serveur.

La base de données 102 du serveur stocke des données permettant à l'ordinateur 100 du serveur de communiquer avec et de traiter les transactions entre l'ordinateur 200 du client et l'ordinateur 300 du commerçant. La figure 4A décrit la structure générale de la base de données 102 du serveur.

Comme représenté en figure 4A, la base de données 102 du serveur comprend une structure 120 de données d'état civil du serveur, une structure 130 des données de la session du serveur, une structure 140 des données du journal de messages, une structure 150 des données de messages et une structure 160 des données de code public et une structure 170 des données d'application. Chacune de ces structures de données sera maintenant décrite en détail.

1. Structure 120 des données d'état civil du serveur.

La structure 120 des données d'état civil du serveur stocke des données concernant l'univers des utilisateurs clients 203 et des utilisateurs commerçants 303 qui ont été inscrits dans l'ordinateur 100 du serveur. En liaison avec la figure 4B, la structure 120 des données d'état civil comprend un ou plusieurs états civils 120.1. On préfère que les états civils des clients 120.1 soient enregistrés en ayant des champs 120A-120H. La structure 120 contient un état civil de client 120.1 pour chaque utilisateur inscrit 203. On décrira maintenant les champs des états civils des clients 120.1.

Le champ 120A stocke un N° d'identification d'état civil pour l'utilisateur client 203. Ce N° d'identification identifie l'utilisateur client particulier 203. Dans le but d'augmenter la sécurité du système, la base de données 102 du serveur ne stocke pas une information pouvant être reconnue pour l'utilisateur client 203. Par exemple, le nom et l'adresse réels de l'utilisateur 203 ne sont pas stockés dans la base de données 102 du serveur. Au contraire, le N° d'identification de l'état civil est utilisé à des fins d'identification. Le champ du N° d'identification de l'état civil est optionnel en ce sens que l'information stockée dans le champ de code public 120C (qu'on décrit

ci-dessous) peut être également utilisée pour localiser des enregistrements associés à l'utilisateur 203. Etant donné qu'un N° d'identification d'état civil est plus court qu'un code public, il est plus efficace, et par conséquent on préfère utiliser le N° d'identification d'état civil à cet effet.

Le champ 120B contient une adresse de protocole de transport de courrier pour l'utilisateur client 203. En utilisant cette adresse du champ 120B, l'ordinateur 100 du serveur est à même d'envoyer ce protocole à l'utilisateur 203 par l'intermédiaire du réseau Internet 50.

Le champ 120C stocke un code public RSA pour l'état civil 120.1. Comme on le décrit pleinement ci-après, le code public RSA du champ 120C est produit par le logiciel 120 d'application du client. Le code public RSA du champ 120C est le composant public d'une paire RSA code public RSA/code privé. Les codes public RSA et privé pour un ordinateur de client 200 sont stockés dans l'ordinateur 200, comme on le décrit ultérieurement. Dans le mode de réalisation ayant la préférence, les codes RSA ont 768 bits de long. Cette longueur reflète un équilibre entre l'augmentation de la sécurité (obtenue en utilisant des codes plus longs) et la diminution des coûts de traitement (qu'on obtient en utilisant des codes plus courts). La puissance du processeur augmentant à l'avenir, des codes RSA plus longs peuvent être utilisés pour accroître la sécurité sans compromettre les performances du système.

Si le code public RSA du client est encapsulé dans un certificat par une autorité de certification appropriée, le code du certificat est utilisé à la place du code public et le champ du N° d'identification 120A de l'état civil n'est plus optionnel comme on l'a décrit précédemment. Des systèmes à base de certificat sont bien connus dans la technique et ne seront pas décrits.

La date que l'utilisateur client 203 a inscrite dans l'ordinateur 100 du serveur est stockée dans le champ 120D. La date du champ 120D permet le passage de promotions (par exemple s'il y a inscription avant cette date, alors cela arrivera) et aide à la résolution des différends.

Le champ 120E contient un langage de communication préféré pour l'utilisateur client 203.

Le champ 120F stocke une phrase de passe d'auto-fermeture pour l'utilisateur client 203. La phrase de passe est une phrase qui permet à l'utilisateur 203 de fermer l'état civil du client 120.1 dans certaines circonstances qu'on décrit ultérieurement.

La donnée 120G représente une structure de données contenant des champs 120G.1-120G.4 représentés en figure 4C. Les champs 120G.1-120G.4 stockent des données pour chaque conteneur d'espèces établi par l'utilisateur client 203. La structure 120 des données d'état civil contient un ensemble de champs 120G.1-120G.4 pour chaque conteneur établi par l'utilisateur 203. Le conteneur d'espèces stocke des espèces électroniques. Il est envisagé d'utiliser de multiples conteneurs d'espèces, par exemple un conteneur pour chaque devise dans laquelle l'utilisateur client 203 a l'intention de faire des affaires.

Les champs 120G.1-120G.4 seront maintenant décrits en détail en liaison avec la figure 4C.

Le champ 120G.1 stocke la devise associée au montant des fonds électroniques stockés dans les champs 120G.2 et/ou 120G.3.

Le champ 120G.2 stocke la balance disponible du conteneur d'espèces.

Le champ 120G.3 stocke la balance en suspens de chaque conteneur d'espèces.

Les espèces électroniques stockées dans les champs 120G.2 et/ou 120G.3 sont de préférence déposées dans un compte d'agence (forme d'instrument bancaire

dans lequel des fonds sont maintenus par un tiers pour le bénéfice de l'autre). Le numéro de ce compte d'agence est stocké dans le champ 120G.4.

La donnée 120H représente une structure de donnée contenant des champs 120H.1-120H.28, représentés en figure 4D. Les champs 120F.1-120H.28 stockent des données pour les instruments liés à l'état civil du client 120.1. La structure 120 des données d'état civil du serveur contient un ensemble de champs 120H.1-120H.28 pour chaque instrument lié à l'état civil 120.1. On décrira maintenant en détail les champs 120H.1-120H.28 en liaison avec la figure 4D.

Le champ 120H.1 stocke le N° d'identification d'état civil du champ 120A (figure 4B). Ce N° d'identification du champ 120H.1 indique l'état civil 120.1 auquel est lié l'instrument ayant les données stockées dans les champs 120H.1-120H.28.

Le champ 120H.2 contient un type d'instrument pour l'instrument lié. Les types d'instruments comprennent de préférence des comptes bancaires, des cartes de débit et des cartes de crédit.

Le champ 120H.3 stocke un sous-type d'instrument pour l'instrument qui est lié. Le sous-type est une sous-classification d'un type d'instrument (par exemple "VISA" pour l'instrument du type carte de crédit").

L'utilisateur client 203 peut choisir d'activer une caractéristique "auto-fermeture" lors de l'inscription de son état civil 120.1. Cette caractéristique permet à l'utilisateur 203 de fournir une phrase de passe (qu'on décrit ultérieurement) pour fermer l'état civil 120.1 et pour décharger toutes les espèces électroniques associées à cet état civil vers un instrument auto-fermé. Si l'instrument qui est lié est l'instrument auto-fermé, le champ 120H.4 contient un numéro d'instrument pour l'instrument qui est lié. Le numéro d'instrument identifie l'instrument. On préfère que le numéro d'instrument soit crypté avant son

stockage. En variante, le numéro d'instrument peut être sauvegardé dans un dispositif de stockage séparé non connecté à l'ordinateur 100 du serveur. Si l'instrument qui est lié n'est pas l'instrument auto-fermé, le numéro de l'instrument est utilisé pour calculer un champ 120H.9 (décrit ultérieurement) et le numéro de l'instrument n'est pas stocké dans le champ 120H.4.

Les instruments qui sont liés peuvent avoir un numéro secondaire identifiant en outre l'instrument lié, par exemple, un numéro CID d'American Express ou de compte CDA-US, R/T. De tels numéros secondaires, qu'on appelle ici des sous-nombres d'instrument, sont stockés dans le champ 120H.5.

Des comptes bancaires sont créés dans une seule devise. La devise indigène d'un instrument de compte bancaire est stockée dans le champ 120H.6.

Le champ 120H.7 stocke un ou plusieurs nombres entiers représentant des accords légaux. Dans le mode de réalisation ayant la préférence, l'opérateur de l'ordinateur 100 du serveur détermine les agréments légaux qui doivent être acceptés par l'utilisateur client 203 pour que cet utilisateur utilise l'instrument lié afin d'effectuer certaines opérations.

Le champ 120H.8 contient un préfixe d'instrument. Le préfixe de 120H.8 est un sous-ensemble du numéro d'instrument décrit en liaison avec le champ 120H.4. Dans le mode de réalisation préféré, le préfixe d'instrument du champ 120H.8 (pour cartes de crédit, cartes de débit, et comptes bancaires) est les deux premier et les quatre derniers chiffres du numéro d'instrument du champ 120H.4.

Le champ 120H.9 stocke une valeur du contrôle de total de somme de l'instrument, de préférence un contrôle de total de somme MD5 pour le numéro de l'instrument qui est décrit en liaison avec le champ 120H.4. (Le terme "contrôle de total de somme" tel qu'il est utilisé dans cette demande concerne des contrôles cryptographiques, par opposition à d'autres

fonctions de contrôle de total de somme mathématiques tels que des contrôles algébriques). Le numéro de l'instrument représenté par le contrôle de total de somme est de préférence rendu plus difficile à deviner en chaînant le numéro de l'instrument avec un nombre aléatoire produit et fourni à l'ordinateur 100 du serveur par l'ordinateur 200 du client (tel qu'un nombre désigné couramment par "sel") avant le contrôle de total de somme. Ce sel est stocké dans le champ 230Q de la structure 230 des données de lien à l'instrument du client comme on le décrit ci-dessous. Le contrôle de total de somme du champ 120H.9 sert à vérifier le numéro de l'instrument sans qu'il soit nécessaire de stocker ce numéro dans l'ordinateur 100 du serveur. Cela réduit l'attraction que présente l'ordinateur 100 comme cible pour des voleurs et des chenapans.

Le champ 120H.10 contient un numéro d'identification de l'émetteur de l'instrument financier lié, appelé également "NIB", ou numéro d'identification de banque.

Si l'instrument financier qui est lié doit être utilisé comme instrument auto-fermé, les champs 120H.11 et 120H.12 contiennent le nom et l'adresse d'un détenteur de l'instrument financier lié. On préfère que cette information soit chiffrée avant stockage. En variante, le numéro de l'instrument peut être sauvegardé dans un dispositif de stockage séparé qui n'est pas relié à l'ordinateur 100 du serveur.

Les champs 120H.13 et 120H.14 stockent des données sur le fait que l'instrument financier a été lié et utilisé en premier lieu, respectivement.

Le champ 120H.15 contient un état d'un instrument financier lié. Le contenu du champ d'état 120H.15 dépend de l'instrument financier qui est lié. Par exemple, pour lier un CDA, l'utilisateur client 203 peut devoir signer un formulaire et autoriser l'opérateur de l'ordinateur 100 du serveur d'enclencher une opération de pré-notification ("pré-note") avec un

établissement de virement automatisé ("EVA"). Avant de recevoir le formulaire signé ou la réponse à la pré-note, l'ordinateur 100 du serveur peut indiquer que le lien a été "créé". Lors de la réception du formulaire signé, le champ d'état 120H.15 peut contenir "pré-note en attente". Si la pré-note est envoyée avant le formulaire signé, le champ 120H.15 peut contenir "signature en attente". Si tous deux ont été reçus et sont acceptables, le champ 120H.15 peut contenir "validé". S'il y a un problème avec l'un ou l'autre, ou si une période de temps spécifiée pour recevoir l'un ou l'autre expire, le champ 120H.15 peut contenir "invalidé". Le champ 120H.15 peut aussi contenir "invalidé" s'il est ultérieurement déterminé que l'instrument financier n'est pas utilisable (par exemple un compte est gelé par une banque). L'état des autres instruments financiers liés dépendra du type d'instrument et des étapes nécessaires pour lier un type d'instrument particulier. Naturellement, l'opération de la pré-note peut être exécutée en ligne.

Le champ 120H.16 est un indicateur signalant si oui ou non l'instrument financier lié est validé pour des transactions de vente. Une transaction de vente concerne le cas où un état civil de client 120.1 est utilisé pour payer quelque chose en utilisant directement un instrument financier lié, comme dans le cas d'une carte de débit.

Si le champ 120H.16 indique que l'instrument lié est validé pour des transactions commerciales, une limite dans la devise choisie (indigène) de l'utilisateur client 203 est stockée dans le champ 120H.17. Si une devise indigène n'existe pas, la limite de la transaction commerciale de 120H.17 est donnée en dollars des Etats-Unis d'Amérique. Une valeur spéciale peut être utilisée pour indiquer qu'il n'y a aucune limite à la transaction commerciale pour l'instrument financier lié. Cette valeur spéciale peut être n'importe quelle valeur qui ne se trouve pas dans l'ensemble des

valeurs acceptables du champ. Par exemple, si la limite du champ 120H.17 est exprimée sous la forme d'un nombre positif, la valeur spéciale peut être une valeur négative.

Le champ 120H.18 est un indicateur signalant si l'instrument financier lié est validé pour des transactions de crédit/retour. Une transaction de crédit/retour est une opération dans laquelle un commerçant crédite l'état civil 120.1 d'un client au lieu de fournir le produit sur lequel l'accord a été réalisé à l'origine.

Si le champ 120H.18 indique que l'instrument financier est validé pour des transactions de crédit/retour, une limite de la devise indigène choisie pour l'utilisateur client, par transaction de crédit/retour, est stockée dans le champ 120H.19. Si une devise indigène n'existe pas, la limite de la transaction crédit/retour du champ 120H.19 est en dollars des Etats-Unis d'Amérique. Une valeur spéciale peut être utilisée pour indiquer qu'il n'y a aucune limite à la transaction crédit/retour pour l'instrument financier, comme on l'a décrit précédemment.

Le champ 120H.20 est un indicateur du fait qu'un instrument financier lié est validé pour des opérations de chargement, comme on l'a décrit précédemment.

Si le champ 120H.20 indique que l'instrument est validé pour des opérations de chargement, une limite est stockée dans le champ 120H.21. La limite de transaction des espèces de chargement du champ 120H.21 représente une limite, dans une devise indigène. S'il n'existe pas de devise indigène, la limite de ladite transaction de champ 120H.21 peut être à défaut des dollars américains. Une valeur spéciale peut être utilisée pour indiquer qu'il n'y a aucune limite de la transaction des espèces de chargement pour l'instrument financier lié comme on l'a décrit précédemment.

Le champ 120H.22 est un indicateur du fait que l'instrument financier lié est validé pour des opérations de déchargement, comme on l'a décrit précédemment.

Si le champ 120H.22 indique que l'instrument financier lié est validé pour des transactions de déchargement d'espèces, une limite pour ces transactions est stockée dans le champ 120H.23. La limite d'une telle transaction du champ 120H.23 représente une limite, en devise indigène. S'il n'existe pas de devise indigène, la limite de la transaction du champ 120H.23 peut à défaut être de préférence des dollars américains. Une valeur spéciale peut être utilisée pour indiquer qu'il n'y a aucune limite de la transaction de déchargement d'espèces pour l'instrument financier lié, comme on l'a décrit précédemment.

Le champ 120H.24 est un indicateur du fait que l'instrument financier lié est désigné ou non comme lien auto-fermé pour l'état civil 120.1 du client. Un tel lien doit avoir son indicateur de la transaction de déchargement (champ 120H.22) validé.

Le champ 120H.25 stocke un nombre d'heures pendant lesquelles s'applique la limite des transactions commerciales stockée dans le champ 120H.17.

Le champ 120H.26 stocke un nombre d'heures pendant lesquelles s'applique la limite des transactions de crédit stockée dans le champ 120H.19.

Le champ 120H.27 stocke un certain nombre d'heures pendant lesquelles s'applique la limite des transactions de chargement d'espèces stockée dans le champ 120H.21.

Le champ 120H.28 stocke un nombre d'heures pendant lesquelles s'applique la limite des transactions de déchargement d'espèces stockée dans le champ 120H.23.

Le champ 120I stocke des accords légaux comme on l'a décrit précédemment.

Alors que la description précédente de l'état civil 120.1 du client a été faite en ce qui

concerne des données relatives à l'utilisateur client 203, on remarquera qu'un utilisateur commerçant 303 possède un état civil 120.2 stocké dans la structure 120 des données d'état civil du serveur. L'état civil 120.2 est représenté en figures 4E, 4F et 4G où les champs 120AA-120HH, 120GG.1-120GG.4, et 120HH.1-120HH.28 correspondent aux champs 120A-120H, 120G.1-120G.4, et 120H.1-120H.28 des figures 4B, 4C et 4D.

2. Structure 130 des donnés de session du serveur.

La structure 130 des données de session du serveur, représentée dans ses grandes lignes en figure 4A, stocke les données associées à une session. On décrira maintenant la structure 130 pour l'utilisateur client 203.

En liaison avec la figure 4H, la structure 130 comprend un ou plusieurs enregistrements 130.1 de la session du client. La structure 130 contient un enregistrement 130.1 pour chaque session active de l'utilisateur client 203.

L'ordinateur 100 du serveur identifie une session par un numéro unique d'identification de session ("id session"). Le numéro d'identification de session est stocké dans le champ 130A.

Les messages échangés entre l'ordinateur 100 du serveur et l'ordinateur 200 du client lors d'une session comprennent des données chiffrées. Le champ 130B contient un code de chiffrement (appelé "code de session"). Le code de session du champ 130B est utilisé par l'ordinateur 100 du serveur pour calculer un code de manière à décrypter les messages chiffrés en provenance de l'ordinateur 200 du client.

Le champ 130C stocke un sel de session, d'une préférence de 8 octets de longueur. Comme on le décrira ci-dessous, les messages échangés à l'intérieur d'une session entre l'ordinateur 100 du serveur,

l'ordinateur 200 du client et l'ordinateur 300 du commerçant ne sont pas authentifiés en utilisant des signatures numériques. Au contraire, les messages échangés à l'intérieur d'une session sont authentifiés par la connaissance du code de session et du sel de session qu'on décrit ci-dessus. Pour assurer que la partie non chiffrée d'un message n'est pas altérée, il est l'objet d'un contrôle de total de somme et la valeur de ce total est incluse dans la partie chiffrée du message. L'utilisation du sel de session du champ 130C donne l'assurance que les valeurs de contrôle de total de somme sont plus sûres.

Dans la présente invention, l'utilisateur client 203 peut faire des transactions commerciales dans une ou plusieurs devises. Le champ 130D indique la dénomination d'une devise (par exemple, le dollar des Etats-Unis d'Amérique) que l'utilisateur client 203 utilisera pendant la session.

Le champ 130E représente un montant maximum d'espèces électroniques (dans la devise du champ 130D) mis à la disposition de l'utilisateur client 203 au début de la session.

Le champ 130F représente un montant d'espèces électroniques (dans la devise du champ 130D) mis à la disposition de l'utilisateur 203 à un instant particulier de la session. La valeur initiale du champ 130F est la valeur stockée dans le champ 130E du montant à l'ouverture. Ensuite, la valeur du montant courant du champ 130F est déterminée en soustrayant chaque montant dépensé pour des produits pendant la session à partir de la valeur précédente de 130F.

Le champ 130G indique une date et le temps auxquels la session a été créée. Le champ 130H indique la date et le temps auxquels la session s'est réellement terminée.

Le champ 130I représente le nombre maximum de fois que l'ordinateur 100 du serveur reconnaîtra

l'utilisation par l'ordinateur 200 du client du code de session du champ 130B.

Le champ 130J représente une durée pendant laquelle le code de session du champ 130B est valable.

Le champ 130K stocke le numéro d'identification d'état civil de l'utilisateur client 203. C'est par l'intermédiaire du numéro d'identification d'état civil du champ 130K qu'une session est associée à un état civil 120.1.

Le champ 130L stocke l'état d'une session associée au numéro d'identification de session dans le champ 130A. L'état est soit "ouvert" soit "fermé".

Le champ 130M stocke une chaîne facultative fournie par l'utilisateur client 203 décrivant la session associée au numéro d'identification de session du champ 130A. Le champ 130M peut contenir une chaîne fournie par l'utilisateur 203 à l'ouverture d'une session et une chaîne fournie à la clôture d'une session.

La donnée de transaction 130N comprend les champs 130N.1-130N.5. Les champs 130N.1-130N.5, représentés en figure 4I, sont maintenus par chaque transaction amorcée par l'utilisateur 203 lors de la session identifiée par le numéro de session du champ 130A. Le nombre maximum de ces transactions est égal à la limite d'utilisation de code stockée dans le champ 130I. Les champs 130N.1-130N.5 seront maintenant décrits en détail en liaison avec la figure 4I.

Le champ 130N.1 contient le montant chargé chez l'utilisateur 203 pour une transaction particulière.

Le champ 130N.2 stocke le numéro d'identification de session stocké dans le champ 130A.

Le champ 130N.3 stocke un numéro d'identification d'ordre ("N° id. d'ordre") produit par l'ordinateur 300 du commerçant pour identifier un ordre particulier.

Le champ 130N.4 stocke le numéro d'identification de session du commerçant 303 auprès duquel le produit associé à une transaction particulière est acheté.

Le champ 130N.5 contient la valeur d'indice affectée par l'ordinateur 200 du client à une transaction particulière. La valeur d'indice doit être comprise dans la limite d'utilisation de code établie comme indiqué dans le champ 130J. Etant donné que les transactions exécutées par l'état civil 120.1 du client peuvent ne pas être reçues par l'ordinateur 100 du serveur dans l'ordre dans lequel elles sont exécutées, la valeur d'indice est stockée d'une certaine manière, telle qu'une mappe de bits de valeurs d'indices permis, qui permet à l'ordinateur 100 du serveur de déterminer si un indice permis a été utilisé et de prendre l'action appropriée dans le cas où cela se produirait.

Alors que la description précédente de la structure 130 des données de la session du serveur, de l'enregistrement 130.1 de la session du client a été faite en ce qui concerne des données relatives à l'utilisateur client 203, on remarquera qu'un utilisateur commerçant 303 a des données correspondantes qui sont stockées dans la structure 130. Un tel enregistrement 130.2 de la session du commerçant est stocké dans les figures 4J et 4K où les champs 130AA-130NN correspondent aux champs 130A-130N, et les champs 130NN.1-130NN.5 correspondent aux champs 130N.1-130N.5.

3. <u>Structure 140 des données du journal de messages</u>.

La structure 140 des données du journal de messages (figure 4A) poursuit les messages reçus et envoyés par l'ordinateur 100 du serveur. Cela permet à l'ordinateur 100 d'identifier les messages en double et de répondre en conséquence. Les messages en double sont utilisés pour assurer un état homogène entre un donneur

d'ordres et l'ordinateur 100 du serveur en vue de communications ne pouvant être prédites par le réseau Internet 50. Par exemple, à un double d'un message valable il pourrait être répondu par une réponse originale. Cependant, l'ordinateur 100 du serveur pourrait ne pas dupliquer le traitement du message en double. Un enregistrement 140.1 de la structure 140 des données du journal de messages sera maintenant décrit en liaison avec la figure 4L.

Le champ 140A contient le numéro d'identification d'état civil inclus dans le message reçu par l'ordinateur 100 du serveur.

Le champ 140B contient le numéro de session inclus dans un message CA2 (décrit ultérieurement) reçu par l'ordinateur 100 du serveur. Pour tous les autres messages reçus par l'ordinateur 100, ce champ est de préférence nul.

Le champ 140C contient le numéro de transaction inclus dans un message R1, RB1, LU1, OS1, ou CS1 (qu'on décrit ultérieurement) reçu par l'ordinateur 100 du serveur. Pour tout message CA2 reçu par l'ordinateur 100, ce champ est de préférence nul.

Le champ 140D contient l'indice inclus dans le message CA2 reçu par l'ordinateur 100. Pour tous les autres messages reçus par l'ordinateur 100, ce champ est de préférence nul.

Le champ 140E contient un contrôle de total de somme, ou une copie, du message reçu par l'ordinateur 100 associé aux champs 140A-140D.

Le champ 140F contient une copie d'un message envoyé par l'ordinateur 100 en réponse au message sauvegardé dans le champ 140E.

4. Structure 150 des données d'un message.

La structure 150 des données d'un message (figure 4a) comprend des grilles représentatives du format et des contenus des messages utilisés dans la présente invention par type et version. Par exemple, un message particulier peut être différent entre une ou plusieurs versions supportées du logiciel d'application 210 du client ou du logiciel d'application 310 du commerçant. Lorsqu'un message est reçu par l'ordinateur 100 du serveur, il est comparé à une grille pour ce message. Comme on le décrit ultérieurement, si le message n'est pas conforme à la grille, un message d'erreur est renvoyé à l'expéditeur du message.

5. Structure 160 des données de code privé.

La structure 160 des données de code privé maintient une liste des paires de codes public/privé RSA de l'ordinateur 100 du serveur qui sont utilisées dans des versions supportées du logiciel d'application 210 du client ou du logiciel d'application 310 du commerçant. Comme on le décrira ultérieurement, des messages cryptés envoyés à l'ordinateur comprennent un pointeur qui indique à l'ordinateur 100 le code public RSA de l'ordinateur 100 qui a été utilisé par le logiciel d'application 210 du client ou par le logiciel d'application 310 du commerçant pour chiffrer le message. De cette manière, l'ordinateur 100 du serveur peut trouver le code privé RSA correspondant afin de décrypter le message chiffré.

6. Structure 170 des données d'application.

La structure 170 des données d'application poursuit la ou les versions existantes du logiciel d'application 210 du client et du logiciel d'application 310 du commerçant. La structure 170 des données

d'application est également utilisée pour déterminer si oui ou non une mise à jour pour le logiciel d'application 210 ou pour le logiciel d'application 310 est disponible ou nécessaire. Par exemple, l'ordinateur 100 du serveur peut indiquer à l'ordinateur 200 du client que le logiciel d'application 210 du client n'est pas encore couramment utilisable, ou que le logiciel n'est plus utilisable et doit être remplacé.

B. Base de données 202 du client.

La figure 5A décrit la structure générale de la base de données 202 du client. La base de données 202 comprend une structure 215 de données d'application du client, une structure 220 de données d'état civil du client, une structure 230 de données du lien à un instrument financier du client, une structure 240 de données de session du client, une structure 250 de données de transaction en attente du client, une structure 260 des données du journal du client, une structure 270 de données de grille de messages et une structure 280 de données sur les espèces du client. Chacune de ces structures sera maintenant décrite en détail.

1. Structure 215 des données d'application du client.

La structure 215 stocke des données relatives à l'ordinateur 100 du serveur. En liaison avec la figure 5B, la structure 215 comprend l'enregistrement 215.1 qu'on décrit ici en détail.

Le champ 215A contient un code public RSA pour l'ordinateur 100 du serveur. Le code public RSA du champ 215A est utilisé par l'ordinateur 200 du client pour chiffrer les données dans des messages envoyés par l'ordinateur 200 du client à l'ordinateur 100 du serveur.

Le champ 215B stocke un releveur de ressources uniformes ("RRU") pour l'ordinateur 100 du serveur. Le RRU du champ 215B est l'adresse de l'ordinateur 100 sur le web mondial du réseau Internet 50.

Alors que la description ci-dessus de la structure 215 des données d'application du client et de l'enregistrement 215.1 a été faite en ce qui concerne des données relatives à l'utilisateur client 203, on remarquera qu'un utilisateur commerçant 303 a des données correspondantes qui sont stockées dans la structure 315 des données d'application du commerçant, représentée en figure 6B. Un enregistrement 315.1 du commerçant est représenté en figure 6B dans laquelle les champs 315A-315B correspondent aux champs 215A-215B.

2. Structure 220 des données d'état civil du client.

La structure 220 des données de l'état civil du client stocke les données relatives à l'utilisateur client 203. En liaison avec la figure 5C, la structure 220 comprend un enregistrement 220.1, qui y est représenté en détail.

Les champ 220A-220C correspondent à et contiennent la même information que les champs 120A-120C (figure 4B).

Le champ 220D stocke une phrase de passe d'auto-fermeture pour l'utilisateur client 203. La phrase est une phrase de passe qui permet à l'utilisateur client 203 de clôturer l'état civil 120.1 du client dans certaines circonstances comme on le décrit ultérieurement.

Le champ 220E contient un langage préféré de communication pour l'utilisateur client 203.

Un nom et une adresse implicites de l'utilisateur client 203 sont stockés dans le champ 220F. Ce nom et cette adresse du champ 220F sont le nom

et l'adresse de la personne individuelle dont l'état civil 120.1 est indiqué par le numéro d'identification d'état civil du champ 220A. Ce nom et cette adresse du champ 220F facilitent la fourniture d'une telle information lorsqu'elle est requise.

Le champ 220G contient les sélections préférées du logiciel d'application 210 du client, par exemple, les préférences en matière de communication (par exemple la plage d'expiration du temps en secondes), les préférences en matière d'alerte (par exemple les alertes avant la soumission des transactions hors-ligne et/ou lors d'un enregistrement), et les préférences en matière de sécurité (par exemple la demande d'un mot de passe avant une opération de paiement).

Le champ 220H stocke le code privé RSA pour un état civil de 120.1 de client. Le code privé RSA du champ 220H est le complément du code public du champ 120C, stocké dans la base de données 102 du serveur.

La donnée 220I du conteneur d'espèces représente les champs 280A-280C indiqués en figure 5U.

Le lien 220J à un instrument financier représente les champs 230A-230S indiqués en figure 5D.

Le champ 220K contient le numéro de compte auto-fermé qui est associé au mot de passe stocké dans le champ 220D.

Le champ 220L stocke un ou plusieurs nombres entiers représentant des accords légaux. Dans le mode de réalisation préféré, l'opérateur de l'ordinateur 100 du serveur détermine les accords légaux qui doivent être suivis par l'utilisateur client 203 pour que cet utilisateur crée un état civil.

La donnée de sessions actives 220M représente les champs 240A-240K.

La donnée de journal en attente 220N représente les enregistrements 251-256 de la structure 250 des données de journal en attente.

La donnée 2200 de journal de transaction représente les enregistrements 261-267 de la structure 260 des données de journal des transactions.

Alors que la description précédente de la structure 220 des données d'état civil de client et l'enregistrement 220.1 ont été expliqués en liaison avec les données relatives à l'utilisateur client 203, on remarquera que l'utilisateur commerçant 303 a des données correspondantes qui sont stockées dans la structure 320 des données d'état civil de commerçant, représentée en figure 6C. L'enregistrement 320.1 de commerçant est représenté en figure 6C dans laquelle les champs 320-3200 correspondent aux champs 220A-2200.

3. Structure 230 des données du lien à un instrument financier du client.

La structure 230 des données du lien à un instrument financier de client contient une information dans l'ordinateur 200 du client concernant les instruments financiers liés. En figure 5D, la structure 230 comprend un ou plusieurs enregistrements 230.1. La base de données 202 du client contient un enregistrement 230.1 pour chaque instrument financier lié à l'état civil 120.1 du client. Un enregistrement détaillé 230.1 d'une structure 230 est représenté en figure 5D dans laquelle :

le champ 230A stocke le numéro d'instrument.

Le champ 230B contient une description de l'instrument lié.

Les champs 230C-230J représentent respectivement le nom, l'adresse, la ville, le pays, le code postal, le code du pays, le code de zone et le numéro de téléphone du détenteur de l'instrument financier lié.

Le champ 230K stocke une devise implicite associée à l'instrument financier lié.

Les champs 230L-230O sont des indicateurs signalant si l'instrument financier lié est validé pour des transactions de ventes, des transactions de retour de crédit, des opérations de chargement et déchargement. Les champs 230L-230O correspondent aux champs 120H.16, 120H.18, 120H.22 et 120H.20, respectivement (figure 4D).

Le champ 230P contient un état de l'instrument financier lié. L'état du lien du champ 230P correspond à l'état du lien du champ 120H.15 de la figure 4D.

Le champ 230Q stocke un "sel" pour l'instrument financier lié. Le sel du champ 230Q représente un nombre aléatoire produit par le logiciel d'application 210 du client. Comme on l'a précédemment décrit, il est utilisé par le serveur pour renforcer le résultat de la valeur de contrôle de total de somme de l'instrument qui est stocké dans le champ 120H.9.

Le champ 230R stocke une certaine information associée à un instrument financier lié et est appelé "donnée récurrente d'instrument". La donnée récurrente est une chaîne de données qui est utilisée par le logiciel d'application 210 du client pour reconstruire un ensemble de paires libellé-valeur identifiées par l'ordinateur 100 du serveur au moment où un instrument financier est l'objet d'un lien. Les champs sont renvoyés à l'ordinateur 100 par l'ordinateur 200 du client pendant des opérations qui nécessitent l'emploi de l'instrument financier associé à la donnée récurrente. De cette façon, l'ordinateur 100 peut recevoir une information relative à l'instrument lorsque cela s'avère nécessaire sans avoir à stocker cette information dans ses structures de données. Les paires libellé-valeur particulières qui sont contenues dans la donnée récurrente dépendent du type de l'instrument lié et des exigences de l'émetteur de l'instrument. Par exemple, une carte de crédit pourrait nécessiter le numéro de carte, la date d'expiration de la carte, et le nom et l'adresse du détenteur de la carte pour les

renvoyer au serveur lors de chaque utilisation de la carte pour charger des fonds dans l'état civil 120.1. La donnée récurrente contiendra une donnée qui permettra au logiciel d'application 210 du client de renvoyer cette information dans le format approprié de la paire libellé-valeur.

Le champ 230S correspond et stocke la même information que le champ 120H.7 (figure 4D) concernant les accords légaux.

Alors que la description précédente de la structure 230 des données de lien à un instrument financier de client et de l'enregistrement 230.1 a été donnée en ce qui concerne des données relatives à l'utilisateur client 203, on remarquera qu'un utilisateur commerçant 303 a des données correspondantes qui sont stockées dans la structure 330 des données de l'état civil du commerçant, représentée en figure 6D. Un enregistrement de commerçant 330.1 est représenté en figure 6D dans laquelle les champs 330A-330S correspondent aux champs 230A-230S.

4. Structure 240 des données d'une session de client.

La structure 240 des données d'une session de client contient une information dans l'ordinateur 200 du client concernant une session. En figure 5E, la structure 240 comprend un ou plusieurs enregistrements 240.1. La structure 240 contient un enregistrement 240.1 pour chaque session active de l'utilisateur client 203. Un enregistrement détaillé 240.1 de la structure 240 est représenté en figure 5E.

Les champs 240A-240F correspondent à et contiennent la même information relative à une session que les champs 130A-130F (figure 4H). Le champ 240G contient le dernier indice utilisé par l'ordinateur 200 du client pendant la session. Le champ 240H contient la même information que le champ 130M. Les champs 240J-240K

contiennent les mêmes données que les champs 130I-130J, respectivement.

Alors que la description précédente de la structure 240 et de l'enregistrement 240.1 a été donnée en ce qui concerne les données relatives à un utilisateur client 203, on remarquera qu'un utilisateur commerçant 303 a des données correspondantes qui sont stockées dans la structure 340 des données d'état civil de commerçant, représentée en figure 6. Un enregistrement de commerçant 340.1 est représenté en figure 6E dans laquelle les champs 340A-340K correspondent aux champs 240A-240K (figure 5D).

5. Structure 250 des données de transaction en attente de client.

La structure 250 des données de transaction en attente de client stocke (1) la donnée nécessaire pour créer des messages envoyés par l'ordinateur 200 du client et (2) une copie de chaque message envoyé par l'ordinateur 200. En figure 5F, la structure 250 comprend les enregistrements suivants : une inscription d'état civil en attente/information de mise à jour d'état civil 251, une liaison en attente/mise à jour de lien d'instrument financier 252, un paiement d'espèces en attente 253, un chargement/déchargement en attente de fonds 254, un enregistrement 255 d'ouverture de session en attente et un enregistrement 256 de clôture de session en attente. Chaque enregistrement 251-256 sera maintenant décrit en détail en liaison avec les figures 5G-5L. On préfère qu'un enregistrement en attente 251-256 soit supprimé lors de la réception par l'ordinateur 200 du client d'un message de réponse sauf indication contraire de l'utilisateur client 203.

a. Inscription en attente d'état civil/ enregistrement d'une information de mise à jour d'état civil 251.

L'inscription d'état civil en attente/ enregistrement d'une information de mise à jour d'état civil 251 stocke une donnée concernant des opérations au moyen desquelles l'utilisateur client 203 crée un état civil de client 120.1. En figure 5G, on représente en détail l'enregistrement 251.

Le champ 251A indique un code qui représente un type d'action en exécution. Par exemple, le champ 251A peut contenir "création" qui indiquera que l'utilisateur 203 crée un état civil 120.1. Si un état civil 120.1 existe déjà et que l'action en exécution consiste à changer quelque chose qui est associée à cet état civil, le champ 251A peut contenir "modification".

Le champ 251B stocke un numéro de transaction, c'est-à-dire un numéro unique qui indique une action particulière. Le numéro de transaction du champ 251B est produit par le logiciel d'application 210 du client. Le numéro de transaction du champ 250B permet à l'ordinateur 100 du serveur d'envoyer un message de réponse associé. Etant donné que les numéros des transactions sont uniques, le numéro de transaction du champ 251B permet aussi à l'ordinateur 100 du serveur de déterminer si un message R1 est un message dupliqué.

Le champ 251C représente la date et l'heure auxquelles le message R1 a été assemblé et envoyé à l'ordinateur 100 du serveur.

Le champ 251D stocke la version du logiciel d'application 210 utilisée pour assembler le message R1. Comme on le décrit en outre ultérieurement, le numéro de version de logiciel du champ 251D est utilisé pour déterminer si le logiciel d'application 210 du client n'est pas à jour.

Le champ 251E contient un langage préféré pour l'utilisateur client 203, qui correspond au champ 220E (figure 5B).

Le champ 251F contient une devise préférée pour l'utilisateur client 203, qui correspond au champ 240D (figure 5D).

Le champ 251G stocke un numéro d'identification d'état civil demandé par l'utilisateur client 203. On remarquera que ce numéro d'identification du champ 251G peut être le même que le numéro d'identification d'état civil du champ 120A qui est finalement affecté à l'utilisateur 203. Par exemple, l'ordinateur 100 du serveur peut rejeter le numéro d'identification d'état civil demandé du champ 251G s'il est déjà utilisé par un autre utilisateur 203.

Le champ 251H contient l'adresse du protocole de transport de courrier pour l'utilisateur client 203, correspondant au champ 220B (figure 5B).

Le champ 251I contient une phrase de passe d'auto-fermeture, correspondant au champ 120F (figure 4A).

Le champ 251J stocke une chaîne de transaction originelle qui est une copie du message originel R1 envoyée par l'ordinateur 200 du client à l'ordinateur 100 du serveur.

b. Enregistrement 252 de lien/mise à jour d'instrument en attente.

L'enregistrement 252 de lien/mise à jour en attente stocke une donnée relative à des opérations par lesquelles l'utilisateur client 203 lie un instrument financier à un état civil de client 120.1 ou met à jour un instrument existant lié. En figure 5H, on représente en détail un enregistrement 252.

Le champ 252A indique un code qui représente un type d'action en cours d'exécution. Par exemple, le champ 252A peut contenir une "liaison" qui indiquera que

l'utilisateur 203 est en train de relier un instrument à l'état civil 120.1 d'un client. Si l'action exécutée consiste à changer quelque chose qui est associée à un instrument déjà relié à cet état civil, le champ 252A peut contenir une "mise à jour".

Les champs 252B-252D correspondent et stockent la même information que les champs 251B-251D de la figure 5G. Ces champs concernent le numéro de transaction, la date et l'heure d'une transaction, et la version du logiciel, respectivement.

Le champ 252E contient le numéro d'identification d'état civil de l'utilisateur client 203, correspondant au champ 220A (figure 5B).

Le champ 252F stocke le numéro de l'instrument financier qui est en train d'être lié à l'état civil 120.1.

Le champ 252G stocke une information supplémentaire sur l'identification du client qui est nécessaire pour utiliser l'instrument financier en train d'être lié, par exemple, le numéro d'identification du client de la carte American Express.

Le champ 252H stocke le nom de la personne au nom de laquelle l'instrument financier en train d'être lié a été émis.

Le champ 252I stocke la date d'expiration de l'instrument lié.

Les champs 252J-252Q stockent respectivement l'adresse de la rue, la ville, l'état, le code postal, le pays, le code du pays, le code de zone et le numéro de téléphone de la personnel au nom de laquelle l'instrument financier a été émis.

Le champ 252R contient la description sélectionnée de l'utilisateur client 203 de l'instrument qui est soumis au lien.

Le champ 252S de la donnée récurrente de l'instrument financier stocke une information stockée dans le champ 230 R comme concernant des instruments ayant été soumis à un lien.

Le champ 252T stocke le type d'instrument financier soumis à un lien, par exemple, VISA, American Express, etc.

Le champ 252U contient un sel de nombre aléatoire, produit par l'ordinateur 200 du client. Le sel du champ 252U est utilisé pour renforcer le contrôle de total de somme du numéro de l'instrument qui est maintenu dans le serveur 100.

Le champ 252V stocke un indicateur qui, s'il est établi, signale que l'instrument est l'instrument d'un compte auto-fermé.

Le champ 252W stocke une chaîne de transactions d'origine qui est la copie du message d'origine BIl envoyé par l'ordinateur 200 du client à l'ordinateur 100 du serveur.

c. Enregistrement 253 d'un paiement comptant en attente.

L'enregistrement 253 d'un paiement comptant en attente stocke une donnée relative à des transactions impliquant des paiements comptants. En figure 5I, on représente en détail un enregistrement 253.

Le champ 253A indique un code qui représente un type d'action en cours d'exécution. Par exemple, si une session est ouverte, le champ 254A peut alors indiquer "paiement comptant", ce qui signifie qu'un utilisateur client 203 envoie un message CAl (qu'on décrit ultérieurement).

Les champs 253B-253D correspondent à et stockent la même information que les champs 251B-251D (figure 5F). Ces champs sont relatifs au numéro de transaction, à la date et à l'heure de la transaction, et à la version du logiciel, respectivement.

Le champ 253E contient le numéro d'identification d'état civil de l'utilisateur client 203, correspondant au champ 220A (figure 5B).

Le champ 253F stocke un numéro d'identification d'ordre ("N° d'id. d'ordre"). Le N° d'id. d'ordre du champ 254F est produit par l'ordinateur 300 du commerçant pour identifier un ordre particulier.

Le champ 253G contient le N° d'id. d'état civil 120AA de l'utilisateur commerçant 303.

Le champ 253H stocke un montant d'espèces électroniques qu'un utilisateur client 203 paye pour un produit qui a été l'objet de la transaction courante.

Le champ 253I fournit un emplacement pour un mémo produit par un utilisateur client optionnel 203 qui décrit cette transaction particulière.

Le champ 253J contient le RRU d'un ordinateur 300 de commerçant auquel le client souhaite envoyer un paiement comptant. Le logiciel d'application 210 du client utilise le champ RRU, 253J, pour diriger des demandes de paiement comptant sous la forme d'un message CA1 à l'ordinateur 300 du commerçant pour acheminement jusqu'à l'ordinateur 100 du serveur.

Le champ 253K stocke le numéro d'identification de la session au cours de laquelle la transaction courante a été amorcée.

Le champ 253L stocke l'indice associé à la transaction courante

Le champ 254M stocke une chaîne de transaction d'origine qui est une copie du message CA1 envoyée par l'ordinateur 200 du client, par l'intermédiaire de l'ordinateur 300 du commerçant, à l'ordinateur 100 du serveur.

d. <u>Enregistrement 254 du chargement/ déchargement de fonds en attente.</u>

L'enregistrement 254 du chargement/ déchargement de fonds en attente stocke une donnée concernant des transactions qui impliquent le chargement et le déchargement d'espèces électroniques. En figure 5J, on représente en détail un enregistrement 254.

Le champ 254A indique un code qui représente un type d'action en cours d'exécution. Par exemple, le champ 254A peut contenir une "charge", ce qui indiquera que le client utilisateur 203 "transfère" des fonds dans le champ 280B du conteneur d'espèces de l'enregistrement 280.1 à partir de l'instrument financier identifié dans le champ 254F. En variante, le champ 254A peut contenir un "déchargement", ce qui indiquera que l'utilisateur client 203 "transfère" des fonds en espèces électroniques à partir du champ 280B du conteneur d'espèces à l'instrument financier identifié dans le champ 254F.

Les champs 254B-254D correspondent à et stockent la même information que les champs 251B-251D (figure 5F). Ces champs concernent le numéro de transaction, la date et l'heure de la transaction, et la version du logiciel, respectivement.

Le champ 254E contient le numéro d'identification d'état civil de l'utilisateur client 203, correspondant au champ 220A (figure 5C).

Le champ 254F stocke un numéro de compte identifiant un instrument lié à partir duquel des fonds doivent être chargés ou dans lequel des fonds doivent être déchargés.

Le champ 254G stocke un montant des fonds devant être chargés ou déchargés dans un instrument lié.

Le champ 254H stocke le type de compte à partir duquel les fonds sont déchargés ou dans lesquel les fonds sont chargés.

Le champ 254I stocke une chaîne de transactions d'origine, qui est une copie du message LU1 envoyé par l'ordinateur 200 du client à l'ordinateur 100 du serveur.

e. Enregistrement 255 d'une ouverture de session en attente.

L'enregistrement 255 d'une ouverture de session en attente stocke une donnée relative à des opérations grâce auxquelles l'utilisateur client 203 crée une session. En liaison avec la figure 5K, on représente en détail un enregistrement 255.

Le champ 255A indique un code qui représente un type d'action en cours d'exécution. Par exemple, le champ 255A peut contenir une "ouverture de session", ce qui indiquera que le client 203 est en train de créer une session.

Les champs 255B-255D correspondent à et stockent la même information que les champs 251B-251D (figure 5F). Ces champs concernent le numéro de transaction, la date et l'heure de la transaction, et la version du logiciel, respectivement.

Le champ 255E contient le numéro d'identification d'état civil de l'utilisateur client 203, correspondant au champ 220A (figure 5C).

Le champ 255F stocke un montant d'espèces électroniques à mettre à disposition lors d'une session.

Le champ 255G stocke une valeur représentant le nombre maximum des transactions que l'utilisateur client 203 peut demander pendant une session.

Le champ 255H stocke une valeur représentant le temps maximum pendant lequel la session restera ouverte.

Le champ 255I stocke le texte d'une description facultative d'une session telle qu'elle est entrée par l'utilisateur client 203.

Le champ 255J stocke la devise associée à la valeur du montant stockée dans le champ 255F.

Le champ 255K stocke une chaîne de transactions d'origine qui est une copie du message OS1 envoyé par l'ordinateur 200 du client à l'ordinateur 100 du serveur.

f. Enregistrement 256 d'une clôture de session en attente.

L'enregistrement 256 d'une clôture de session en attente stocke une donnée relative à des opérations grâce auxquelles un utilisateur client 203 ferme une session. En figure 5L, on représente en détail un enregistrement 256.

Le champ 256A indique un code qui représente un type d'action en cours d'exécution. Par exemple, le champ 256A peut contenir une "clôture de session", ce qui indiquera que le client utilisateur 203 est en train de fermer une session.

Les champs 256B-256D correspondent à et stockent la même information que les champs 251B-251D (figure 5F). Ces champs concernent le numéro de transaction, la date et l'heure de la transaction, et la version du logiciel, respectivement.

Le champ 256E contient le numéro d'identification de l'état civil de l'utilisateur client 203, correspondant au champ 220A (figure 5C).

Le champ 256F contient soit "oui" soit "non". La valeur du champ 257 procède à la détermination du fait que l'utilisateur client 203 a choisi de recevoir un journal des transactions amorcées par l'utilisateur 203 pendant la session devant être fermée.

Le champ 256G stocke le numéro d'identification de session de la session ouverte devant être fermée. En variante, si toutes les sessions ouvertes doivent être fermées, le champ 256G restera nul.

Le champ 256H stocke le texte d'un message en option relatif à la clôture de la session tel qu'il est entré par l'utilisateur client 203.

Le champ 256I stocke une chaîne de transactions d'origine qui est une copie du message CS1 envoyé par l'ordinateur 200 du client à l'ordinateur 100 du serveur.

6. Structure 260 des données du journal du client.

En figure 5A, une structure 260 des données du journal du client maintient une copie de chaque message reçu par l'ordinateur 200 du client. La structure 260 stocke une donnée reçue par l'ordinateur 200 du client qui provient de l'ordinateur 100 du serveur. En figure 5M, la structure 260 comprend les enregistrements suivants : réponse 261 à une inscription d'état civil/information de mise jour d'état civil, réponse 262 de mise en liaison/mise à jour au lien d'un instrument financier, réponse 263 à un paiement en espèces, réponse 264 à un chargement/déchargement de fonds, réponse 265 à une ouverture de session, demande de paiement 266 et réponse 267 à une clôture de session. On décrira maintenant en détail chaque enregistrement 261-267 en liaison avec les figures 5N-5U.

a. Enregistrement 261 d'une information sur une incription d'état civil/réponse à une mise à jour d'état civil.

L'enregistrement 261 d'une information sur l'inscription d'un état civil/mise à jour d'un état civil stocke une donnée relative à la réponse de l'ordinateur 100 du serveur à une demande de création d'un état civil de client 120.1 par l'utilisateur client 203. En figure 5N, on représente en détail un enregistrement 261.

Le champ 261A indique un type d'action qui a été demandée et est identique à la valeur du champ 251A de l'enregistrement 251. L'enregistrement 261B stocke un numéro de transaction qui est le même que la valeur stockée en 251B.

Le champ 261C représente la date et l'heure de l'assemblage du message R1 et de l'envoi à l'ordinateur 100 du serveur.

Comme on le discutera ultérieurement, les messages provenant de l'ordinateur 200 du client et allant à l'ordinateur 100 du serveur acheminent un code contenant le numéro de version du logiciel d'application 210 du client qui est utilisé pour créer le message. A l'ordinateur 100 du serveur, chaque version du logiciel est associée à l'un des trois élibellés "d'état" : courant, avertissement, ou fatal. L'ordinateur 100 vérifie la version du logiciel indiquée dans les messages du client et comprend dans son message de réponse l'un des trois libellés d'état possibles. Le libellé d'état renvoyé dans le message R2 est stocké dans le champ 261D de sévérité du logiciel. Un message de texte concernant le contenu du champ de sévérité 261D peut être également renvoyé par l'ordinateur 100 du serveur et, dans ce cas, est stocké dans le champ 261E.

Un code représentant le succès ou l'échec du message R1 est renvoyé par l'ordinateur 100 du serveur et est stocké dans le champ 261F du code de réponse. Un message en texte concernant le contenu du champ 261F, s'il est envoyé par l'ordinateur 100 du serveur, est stocké dans le champ 261G.

Le champ 261H stocke un numéro d'identification d'état civil demandé par l'utilisateur client 203. Comme on le décrit ci-dessous, si le numéro d'identification demandé est en service, l'ordinateur 100 du serveur suggérera un numéro d'identification d'état civil pour l'utilisateur client 203. Le numéro d'identification suggéré par l'ordinateur 100 est stocké dans le champ 261I.

Le champ 261J contient l'adresse du protocole de transport de courrier pour l'utilisateur 203 qui correspond au champ 220B (figure 5C).

Le champ 261K contient un langage préféré pour l'utilisateur 203, correspondant au champ 220E (figure 5D).

Le champ 261L contient une devise préférée pour l'utilisateur client 203, correspondant au champ 240D (figure 5E).

b. Enregistrement 262 d'une réponse de liaison/mise à jour d'un instrument financier.

L'enregistrement 262 d'une liaison/mise à jour d'instrument financier stocke une donnée relative à la réponse par l'ordinateur 100 du serveur à une demande de l'utilisateur client 203 de procéder au lien d'un instrument financier à un état civil de client 120.1. En figure 5O, on représente l'enregistrement 262 en détail.

Le champ 262A indique un type d'action qui a été demandé et est le même que la valeur du champ 252A de l'enregistrement 252.

Les champs 262B-262G correspondent à et stockent la même information que le champ 261B-261G de la figure 5N. Ces champs concernent la date et l'heure de la transaction, le code de sévérité du logiciel, le message du logiciel, le code de réponse, et le message de réponse, respectivement.

Le champ 262H contient le numéro d'identification d'état civil de l'utilisateur client 203, correspondant au champ 220A (figure 5C).

Le champ 262I stocke le numéro de l'instrument qui est en cours de lien dans l'état civil de client 120.1. Le champ 262J stocke le type d'instrument en cours de lien, par exemple, VISA, American Express, etc., pour l'état civil de client 120.1.

Le champ 262K stocke le nom de la personne pour laquelle l'instrument financier lié a été émis.

Le champ 262L stocke la date d'expiration de l'instrument qui est lié.

Les champs 262M-262U stockent respectivement l'adresse de la rue, la ville, l'état, le code postal, le pays, le code du pays, le code de zone et le numéro de téléphone de la personne pour laquelle l'instrument financier lié a été émis.

Le champ 262V stocke le texte de la description de l'instrument financier qui est lié tel qu'il est entré par l'utilisateur client 203.

Le champ 262W stocke la devise indigène, si elle est associée à un instrument financier qui est renvoyé par l'ordinateur 100 du serveur.

Le champ 262X stocke le nom de l'émetteur de l'instrument financier qui est renvoyé par l'ordinateur 100 du serveur.

Le champ 262Y stocke le pays d'émission de l'instrument financier.

Le champ 262Z stocke un indicateur qui, s'il est établi, signale que l'instrument est l'instrument financier du compte auto-fermé.

c. Enregistrement 263 de réponse à un paiement en espèces.

L'enregistrement 263 de réponse à un paiement en espèces stocke la donnée relative à des transactions impliquant des paiements en espèces et aux sessions. En figure 5P, on représente en détail un enregistrement 263.

Le champ 263A indique un type d'action qui a été demandé et est identique à la valeur du champ 253A de l'enregistrement 253.

Les champs 263B-263E correspondent à et stockent la même information que le champ 261B-261C et 261F-261G de la figure 5N. Ces champs concernent un numéro de transaction, une date et une heure, un code de réponse, et un message de réponse, respectivement.

Le champ 263F contient le numéro

d'identification d'état civil de l'utilisateur client 203, correspondant au champ 220A (figure 5C).

Le champ 263G stocke un numéro d'identification d'ordre ("N° id. d'ordre"). Le N° id. d'ordre du champ 263I est produit par l'ordinateur 300 du commerçant pour identifier un ordre particulier.

Le champ 263H contient un numéro d'identification d'état civil 120AA de l'utilisateur commerçant 303.

Le champ 263I fournit un emplacement pour stocker un message en provenance de l'utilisateur commerçant 303.

Le champ 263J stocke une quantité d'espèces électroniques qu'un utilisateur client 203 paye pour un produit qui a été l'objet de la transaction courante.

Le champ 263K fournit un emplacement pour un mémo produit en option par un utilisateur client 203.

Le champ 263L stocke le numéro d'identification de la session au cours de laquelle la transaction courante a été amorcée.

Le champ 263M stocke l'indice associé à la transaction courante.

d. Enregistrement 264 de la réponse à un chargement/déchargement de fonds.

L'enregistrement 264 de la réponse à un chargement/déchargement de fonds stocke une donnée relative à la réponse de l'ordinateur 100 du serveur à une demande de chargement ou de déchargement de fonds par l'utilisateur client 203. En figure 5Q, on représente en détail un enregistrement 264.

L'enregistrement 264A indique un type d'action qui a été demandée et est identique à la valeur du champ 254A de l'enregistrement 254.

Les champs 264B-264G correspondent à et stockent la même information que le champ 261B-261G de la figure 5N. Ces champs concernent la date et l'heure

de la transaction, le code de sévérité du logiciel, le message du logiciel, le code de réponse, et le message de réponse, respectivement.

Le champ 264H contient le numéro d'identification de l'état civil de l'utilisateur client 203, correspondant au champ 220A (figure 5B).

Le champ 264I stocke un numéro de compte identifiant un instrument financier lié à partir duquel des espèces électroniques doivent être chargées ou dans lequel des espèces électroniques doivent être déchargées.

Le champ 264J stocke un montant d'espèces électroniques devant être chargé ou déchargé dans un instrument lié.

Le champ 264K stocke un montant d'un honoraire quelconque chargé par l'opération de l'ordinateur 100 du serveur afin de charger ou de décharger des fonds à partir de l'état civil 120.1 du client.

Le champ 264L stocke un montant égal à la balance disponible des fonds détenus par l'état civil 120.1 tel qu'il est déterminé par l'ordinateur 100 du serveur, correspondant à la valeur stockée dans le champ 120G.2 (figure 4C).

Le champ 264M stocke un montant des fonds qui ont été chargés (ou déchargés), mais non disponibles pour l'utilisateur client 203. Ces fonds sont en attente de traitement, correspondant à la valeur stockée dans le champ 120G.3 (figure 4C).

e. Enregistrement 265 de la réponse à une ouverture de session.

L'enregistrement 265 de réponse à la création d'une session stocke une donnée concernant la réponse de l'ordinateur 100 du serveur à une demande de création d'une session par l'utilisateur client 203. En figure 5R, on représente en détail l'enregistrement 265.

Le champ 265A indique un type d'action qui a été demandée et est identique à la valeur du champ 255A de l'enregistrement 255.

Les champs 265B-265G correspondent à et stockent la même information que le champ 261B-261G de la figure 5N. Ces champs concernent la date et l'heure de la transaction, le code de sévérité du logiciel, le message du logiciel, le code de réponse, et le message de réponse, respectivement.

Le champ 265H concerne le numéro d'identification de l'état civil de l'utilisateur client 203, correspondant au champ 220A de la figure 5C.

Le champ 265I stocke un montant des espèces électroniques rendues disponibles au cours d'une session.

Le champ 265J stocke une valeur représentant le nombre maximum des transactions que l'utilisateur client 203 peut demander au cours d'une session.

Le champ 265K stocke une valeur représentant le temps maximum pendant lequel la session restera ouverte.

Le champ 265L stocke le numéro d'identification d'une session.

Le champ 265M stocke le texte d'une description facultative de la session devant être ouverte tel qu'il est entré par l'utilisateur client 203.

Le champ 265N stocke le montant d'un honoraire chargé par l'opération de l'ordinateur 100 du serveur pour créer une session.

Le champ 265O stocke la balance disponible qui reste dans le conteneur d'espèces (champ 120G.2) après la soustraction de la valeur dans le champ de montant 265I.

f. Enregistrement 266 d'une demande de paiement.

L'enregistrement 266 d'une demande de paiement stocke une donnée concernant une demande provenant de l'utilisateur commerçant 303 pour le paiement du produit. La demande se présente sous la forme d'un message PR1 (qu'on décrit ultérieurement) qui est envoyée par l'ordinateur 300 du commerçant à l'ordinateur 200 du client. En figure 5S, on représente en détail l'enregistrement 266.

Le champ 266A contient le numéro d'identification 120AA de l'état civil de l'utilisateur commerçant 303.

Le champ 266B stocke un numéro d'identification d'ordre ("N° d'id. d'ordre"). Le N° d'id. d'ordre du champ 266B est produit par l'ordinateur 300 du commerçant pour identifier un ordre particulier.

Le champ 266C stocke un montant d'espèces électroniques qu'un utilisateur client 203 paye pour le produit qui est l'objet de la transaction courante.

Le champ 266D stocke une liste de cartes de crédit acceptées par le commerçant 203 pour paiement.

Le champ 266E fournit un emplacement pour le stockage d'un message provenant de l'utilisateur commerçant 303.

Le champ 266F stocke le "à payer à RRU". La valeur de la paire libellé-valeur 5013I est un releveur de données des ressources uniformes du réseau Internet 50. Ce releveur de ressources de la paire 5013I est l'adresse sur le réseau Internet 50 à laquelle l'ordinateur 200 du client doit envoyer le message CA1 qu'on décrit ultérieurement.

g. Enregistrement 267 de la réponse à une clôture de session.

L'enregistrement 267 de la réponse à une clôture de session stocke la donnée concernant la réponse à l'ordinateur 100 du serveur à une demande de clôture de la session par l'utilisateur client 203. En figure 5T, on représente en détail l'enregistrement 267.

Le champ 267A indique le type d'action qui a été demandée et est identique à la valeur du champ 256A de l'enregistrement 256.

Les champs 267B-267G correspondent à et stockent la même information que le champ 261B-261G de la figure 5N. Ces champs concernent la date et l'heure de la transaction, le code de sévérité du logiciel, le message du logiciel, le code de réponse, et le message de réponse, respectivement.

Le champ 267H contient le numéro d'identification d'état civil de l'utilisateur client 203, correspondant au champ 220A (figure 5C).

Le champ 267I stocke le montant des espèces électroniques restant dans la session après la clôture d'une session alors que tous les paiements et honoraires ont été déduits.

Le champ 267J stocke le journal des transactions renvoyé par l'ordinateur 100 du serveur s'il a été demandé par l'utilisateur client 203 dans un message CS1. Cela indiquera aussi si oui ou non un journal des transactions a été renvoyé.

Le champ 267K stocke le montant de tout honoraire chargé par l'opération de l'ordinateur 100 du serveur pour clore la session.

7. Structure 270 des données de grille de messages.

En figure 5A, une structure 270 des données de grille des messages trace le format et les contenus

des messages que l'utilisateur client 203 envoie et reçoit. Un message qui contient tous les libellés requis avec des valeurs valables (par exemple syntaxe, etc.), tels qu'ils sont déterminés par référence à la structure 270 sera traité même s'il y a des paires libellé-valeur étrangères. Un message qui ne contient pas la totalité des paires libellé-valeur requises, ou qui comprend des libellés associés à des valeurs non valables telles qu'elles sont déterminées par référence à la structure 270 ne sera pas formé.

Alors que la description ci-dessus des grilles de messages 270 a été donnée en ce qui concerne une donnée relative à l'utilisateur client 203, on remarquera qu'un utilisateur commerçant 303 a une donnée correspondante qui est stockée dans les grilles de messages 380, comme représenté en figure 6A.

8. Structure 280 des données de conteneur d'espèces.

La structure 280 des données de conteneur d'espèces du client conserve une information à l'ordinateur 200 du client qui concerne les conteneurs d'espèces. En figure 5U, chaque structure 280 contient un enregistrement 280.1 pour chaque conteneur d'espèces établi par l'utilisateur client 203. Un enregistrement détaillé 280.1 de la structure 280 est représenté en figure 5U.

Les champs 280A-280C correspondent à et contiennent la même information relative à un conteneur d'espèces que les champs 120G.1-120G.3 (figure 4C).

Alors que la description précédente de la structure 280 et de l'enregistrement 280.1 a été donnée en ce qui concerne une donnée relative à un utilisateur client 203, on remarquera qu'un utilisateur commerçant 303 a une donnée correspondante qui est stockée dans la structure 345 des données du conteneur d'espèces du commerçant, représentée en figure 6F. Un enregistrement

345.1 du commerçant est représenté en figure 6F dans laquelle les champs 345A-345C correspondent aux champs 280A-280C (figure 5U).

C. Base de données de commerçant 305.

On décrira maintenant la base de données 305 de l'ordinateur 300 du commerçant.

La figure 6A représente la structure générale de la base de données 305 de l'ordinateur 300 du commerçant. La figure 6A représente la structure 315 des données d'application du commerçant (qu'on a décrite précédemment), la structure 320 des données de l'état civil du commerçant (qu'on a décrite précédemment), la structure 330 des données du lien à l'instrument financier du commerçant (qu'on a décrite précédemment), la structure 340 des données de session du commerçant (qu'on a décrite précédemment), la structure 350 des données du montant du commerçant, la structure 360 des données de la session des ventes du commerçant, le journal 370 des espèces du commerçant, la structure 380 des données de la grille de messages (qu'on a décrite précédemment), et la structure 345 des données du conteneur des espèces du commerçant (qu'on a décrite précédemment). On décrira maintenant les structures de données 350, 360 et 370.

1. Structure 250 des données du montant du commerçant.

La structure 350 des données du montant du commerçant suit le montant des espèces électroniques que l'utilisateur commerçant 303 s'attend à recevoir de la part de l'utilisateur client 203 pour un ordre. En figure 7A, on représente en détail l'enregistrement 350.

Le champ 350A stocke un numéro d'identification d'ordre, correspondant au champ 253F de la figure 5I.

Le champ 350B stocke un montant des espèces électroniques correspondant au champ 253H de la figure 5I.

Le champ 350C est un indicateur signalant si un ordre a été payé pour l'utilisateur client 203.

2. Structure 360 des données d'une session de ventes du commerçant.

La structure 360 les données d'une session de ventes du commerçant suit les sessions de l'utilisateur commerçant 303. En figure 7B, on représente en détail l'enregistrement 360.

Les champs 360A-360D correspondent aux champs 340A-340D (figure 6E). Le champ 360E correspond au champ 340H (figure 6E). Les champs 360G correspondent au champ 340F (figure 6E). Les champs 360J-360K correspondent aux champs 340J-340K (figure 6E). Le champ 360 G stocke la date à laquelle la session des ventes du commerçant identifiée par le champ d'identification de session 360A a été ouverte. Le champ 360 H stocke la date de la clôture d'une telle session.

3. Structure 370 des données du journal des espèces du commerçant.

Le journal 370 des espèces du commerçant suit les transactions des espèces électroniques et des données de session non conservées dans la structure 360 des données d'une session de ventes du commerçant. Plus spécialement, la structure 370 stocke une donnée concernant des collectes et des sessions amorcées par l'utilisateur commerçant 303. En figure 7C, on représente en détail un enregistrement 370.

Les champs 370A-370M stockent une donnée concernant les messages de collecte CA2 soumis par l'ordinateur 300 du commerçant à l'ordinateur 100 du serveur. On décrit maintenant en détail ces champs.

Le champ 370A indique un type d'action en cours d'exécution. Dans ce cas, le type stocké dans le champ 370A est "collecte".

Le champ 370B stocke l'état de la demande de collecte courante. L'état du champ 370B peut comprendre "tentative", "succès" ou "échec". Le libellé "tentative" sera retourné lorsque la demande a été envoyée à l'ordinateur 100 du serveur mais qu'aucune réponse n'a été reçue. Si la demande est traitée par l'ordinateur 100 et que la demande de collecte est honorée, le champ 370B contiendra le libellé "succès". Si l'ordinateur 100 refuse la demande, le champ 370B contiendra le libellé "échec" et le champ 370M comprendra un code identifiant la raison d'un tel échec.

Le champ 370C stocke un numéro d'identification d'ordre ("N° d'id. d'ordre"). Le N° d'id. d'ordre du champ 370A est produit par l'ordinateur 300 du commerçant afin d'identifier un ordre particulier.

Le champ 370D stocke le numéro d'identification de session du champ 240A utilisé par l'ordinateur 200 du client dans la demande courante de collecte.

Le champ 370E stocke l'indice du champ 240G utilisé par l'ordinateur 200 du client dans la demande de collecte courante.

Le champ 370F stocke la devise du champ 240D utilisée par l'ordinateur 200 du client dans la demande de collecte courante.

Le champ 370G stocke le numéro d'identification de session du champ 340A utilisé par l'ordinateur 300 du commerçant dans la demande de collecte courante.

Le champ 370H stocke l'indice de la paire libellé-valeur 5213D utilisée par l'ordinateur 300 du commerçant dans la demande de collecte courante.

Le champ 370I stocke la devise du champ 340D utilisée par l'ordinateur 300 du commerçant dans la demande de collecte courante.

Le champ 370J stocke le montant des fonds en espèces électroniques dont le paiement a été demandé pour l'utilisateur commerçant 303 dans la demande de collecte courante.

Le champ 370K stocke le montant des espèces électroniques crédité dans le champ 345B du conteneur des espèces du commerçant pour la collecte courante. Le montant des espèces électroniques crédité est nul si l'état du champ 370B est nul.

Le champ 370L stocke un montant des fonds en espèces électroniques payés à l'opérateur de l'ordinateur 100 du serveur pour traiter la demande de collecte courante.

Si le contenu du champ d'état 370B est "échec", le champ 370M stocke un code de résultat. Le code de résultat est utilisé par le logiciel d'application 310 du commerçant pour associer un message à l'échec signalé dans le champ d'état 370B. Ainsi, le code retourné dans le champ 370M pourrait amener le logiciel d'application du commerçant à afficher un message tel que "échec de collecte à cause de fonds inadéquats".

Les champs 370N-370T stockent une donnée concernant des sessions amorcées par l'ordinateur 300 du commerçant (message OS1). On décrira maintenant en détail ces champs.

Le champ 370N indique un type d'action en cours d'exécution. Dans ce cas, le type stocké dans le champ 370N est un "OS".

Le champ 370O stocke un état de la demande de collecte courante. L'état du champ 370O peut comprendre "tentative", "succès" ou "échec". Le libellé "tentative" sera retourné lorsque la demande a été envoyée à l'ordinateur 100 du serveur mais qu'aucune réponse n'a été reçue. Si la demande est traitée par

l'ordinateur 100 et que la demande de collecte est honorée, le champ 3700 contiendra le libellé "succès". Si l'ordinateur 100 refuse la demande, le champ 3700 contiendra le libellé "échec" et le champ 370T comprendra un code identifiant la raison d'un tel échec.

Le champ 370P stocke un numéro de transaction, c'est-à-dire un nombre unique représentatif d'une session particulière amorcée par l'ordinateur 300 du commerçant.

Le champ 370Q stocke une valeur du temps demandée par l'utilisateur commerçant 303 que doit durer la session courante.

Le champ 370R stocke le nombre de fois demandé par l'utilisateur commerçant 303 selon lequel le code de session du champ 370J peut être utilisé

Si l'état du champ 3600 est "succès", le champ 370S stocke un numéro d'identification de session pour l'ordinateur 300 du commerçant pour la session courante.

Si le contenu du champ d'état 3700 est "échec", le champ 370T stocke un code de résultat. Le code de résultat est utilisé par le logiciel d'application 310 du commerçant pour associer un message à l'échec rapporté dans le champ d'état 370T.

III. Information générale.

On décrira maintenant le format préféré des messages qu'on utilise dans la présente invention.

Par suite de la nature du réseau Internet 50, la présente invention utilise un mécanisme indépendant pour la transmission des messages de sorte que les messages peuvent être transmis en utilisant plusieurs protocoles différents. Ces protocoles peuvent comprendre un courrier-e (protocole de transport de courrier simple) et un web mondial (protocole de transport hyper-texte ou autres protocoles tels que le protocole de mode opératoire à distance (RPC)). Par

conséquent, les messages utilisés dans la présente invention ont un format particulier et préféré qui n'est pas spécifique au protocole de transport. Le format particulier et préféré est basé sur le RFC 822, qu'on connaît dans la technique et par conséquent, qu'on ne décrit que brièvement.

La figure 7D décrit le format d'un message échantillon 4000. Le message échantillon 4000 comprend un en-tête 4005, un corps 4010 et une queue 4050. Le corps 4010 comprend des paires libellé-valeur (non cryptées) 4013A, 4013B, etc., et peut comporter une paire libellé-valeur (chiffrée) opaque 4017. (Les paires libellé-valeur sont constituées d'un libellé et d'une donnée relative au libellé, séparés par un terminateur de libellé, par exemple, "nom : Brian").

L'en-tête 4005 définit le commencement du message échantillon 4000. L'en-tête 4005 peut comprendre un identificateur de système, par exemple, "CyberCash" (le cessionnaire de la présente invention) et un numéro de protocole de message ("numéro de protocole") dans lequel le message échantillon 4000 a été assemblé.

Les paires transparentes libellé-valeur 4013A, 4013B, etc., comprennent tout texte en clair (non chiffré) associé au message échantillon 4000. On décrit ci-dessous le cryptage et le décryptage.

La paire libellé-valeur opaque 4017 comprend le libellé "opaque". La valeur de la paire 4017 est un bloc de données chiffrées. La valeur de la paire 4017 comprend un ensemble donnée de paires libellé-valeur chiffrées avec un code DES. Après chiffrement, la valeur est de préférence codée sur la base 64. L'ensemble donné de paires libellé-valeur est désigné ici par "contenus de la section opaque" du message échantillon 4000. Pour les messages de demande envoyés à l'extérieur d'une session (R1, BI1, LU1 et CS1), la valeur 4017 de la paire libellé-valeur opaque commence avec ce code DES, chiffré en RSA sous un code RSA public de l'ordinateur 100 du serveur. Le chiffrement RSA est cher en matière

de calcul. Pour les messages de réponse (R2, BI4, LU2, OS2 et CS2) et les messages à l'intérieur d'une session (CA1, CA2, CA3 et CA4), aucune information additionnelle, au-delà des contenus de la section opaque, n'est nécessaire dans la valeur de la paire libellé-valeur opaque 4017, ce qui évite le coût d'un chiffrement RSA. Les contenus de la section opaque varient en longueur et représentent les données chiffrées avec le code DES utilisé.

La queue 4050 comprend le message échantillon 4000. La queue 4050 comporte de préférence un total de contrôle de transmission. On préfère que le total de contrôle de transmission du champ 4050D soit un contrôle de total de somme MD5 exécuté sur tous les caractères imprimables de l'en-tête 4005 et sur ceux apparaissant dans le corps 4010. Ainsi, tous les espaces blancs, dont les lignes nouvelles, les espaces, les retours de chariot, etc., sont omis dans le contrôle de total de somme. De cette manière, l'exactitude de la transmission du message peut être contrôlée tout en évitant la sensibilité aux modules d'adaptation ou au traitement qui pourraient, par exemple, changer la séquence du terminateur de ligne ou convertir les tabulations en espaces.

Les techniques de chiffrement et de décryptage qu'on utilise dans la présente invention seront maintenant décrites.

La présente invention utilise de préférence les méthodes RSA ainsi que DES pour le chiffrement et le décryptage des données. De telles méthodes sont bien connues dans la technique. RSA est totalement décrit dans le brevet des Etats-Unis d'Amérique N° 4 405 829. La présente invention table de préférence sur les codes RSA de 768 bits, qui reflète un équilibre entre les soucis relatifs à la sécurité, le temps d'exécution, et le contrôle de l'exportation. La taille du code RSA peut changer lorsque les ordinateurs avec des vitesses de traitement rapides prévalent dans les installations des

clients et que les exigences en matière d'exportation sont relaxées. Comme cela est connu de l'homme de l'art, d'autres systèmes de codes public/privé asymétriques (tels que les systèmes Rabin et ElGamal) pourraient être utilisés dans la présente invention à des fins d'authentification.

Dans la présente invention, les signature numériques sont utilisées pour identifier l'information. Les détails des signatures numériques sont largement discutés dans la littérature relative à la sécurité des ordinateurs. La présente invention utilise deux méthodes d'authentification : les signatures numériques RSA/MD5 et la connaissance de l'information partagée (par exemple valeur de sel et/ou valeur de code).

Comme on l'a indiqué ci-dessus, la présente invention dépend aussi du contrôle du total de somme des données. Ce contrôle est de préférence calculé en utilisant l'algorithme MD5 bien connu qui est décrit dans la publication Internet, RFC 1321, appliqué à un "message synthétique".

Si une paire libellé-valeur est spécifiée dans une entrée de contrôle de total de somme, mais n'est pas présente dans un message, le libellé et le terminateur de libellé peuvent être de préférence omis dans ce contrôle.

IV. Opérations de la présente invention.

A. Opération 400 de transfert et d'installation.

Pendant l'opération 400 de transfert et d'installation, comme on l'a décrit précédemment en liaison avec la figure 3A, un code public RSA de l'ordinateur 100 du serveur est stocké dans le champ 215A de la structure 215 des données d'application du client. L'ordinateur 300 du commerçant obtient une copie du logiciel d'application 153 de l'utilisateur de la même manière que l'utilisateur client 203 lorsqu'il

utilise l'opération 400 de transfert et d'installation. Dans ce cas, le logiciel 153 réside sur l'ordinateur 300 du commerçant comme composant du logiciel d'application 310 du commerçant et un code public RSA de l'ordinateur 100 du serveur est stocké dans le champ 315A de la structure 315 des données d'application du commerçant.

B. Opération d'inscription 401.

La figure 8 décrit un organigramme représentant l'opération d'inscription 401 qui commence à l'étape 1201.

A l'étape 1202, le logiciel d'application 210 du client indique à l'utilisateur client 203 d'entrer une information concernant cet utilisateur. Cette information sera comprise dans le message R1 envoyé à l'ordinateur 100 du serveur et elle fera partie de l'état civil 120.1 du client. Dans le mode de réalisation préféré, l'utilisateur client 203 entre un langage de communication préféré, une devise dans laquelle les transactions seront traitées, un numéro d'identification d'état civil demandé, une adresse de protocole de transport de courrier et une phrase de passe d'auto-fermeture.

A l'étape 1202A, le logiciel d'application 210 du client produire une paire de codes public/privé RSA pour l'ordinateur 200 du client. Le code public RSA est stocké dans le champ 220C de la structure 220 des données d'état civil du client (figure 5C). Le code privé RSA est stocké dans le champ 220H de la structure 220 (figure 5C).

A l'étape 1203, le message R1 est assemblé en conformité avec l'opération 800 d'assemblage de message, décrite en figure 9. Le message R1 sera envoyé de l'ordinateur 200 du client à l'ordinateur 100 du serveur et comprendra l'information entrée par l'utilisateur client 203 à l'étape 1202. L'opération 800

d'assemblage de message sera maintenant décrite en liaison avec la figure 9.

L'opération 800 de l'assemblage d'un message commence à l'étape 801. Les étapes 802A-802B créent des paires libellé-valeur transparentes 4213A-4213D du message R1, représentées en figure 10A. Les étapes 802C-813 créent une paire libellé-valeur opaque 4217 du message R1, sur la base des contenus de la section opaque du message R1, qu'on représente en figure 10B. Les étapes 814-817 assemblent l'en-tête 4205, les paires libellé-valeur transparentes 4213A-4213D, la paire libellé-valeur opaque 4217 et la queue 4250 du message R1.

A l'étape 802A, le logiciel d'application 210 du client accède à la structure 270 des données de la grille de messages (figure 5A) pour obtenir une liste de libellés, qui, lorsqu'ils sont adaptés aux valeurs associées, constituent les paires libellé-valeur transparentes 4213A-4213C du message R1. A l'étape 802B des valeurs sont associées à chaque libellé de la manière suivante :

La paire libellé-valeur 4213A comporte le libellé "transaction". La valeur du champ 4213A est un numéro de transaction, produit par le logiciel 210 du client, qui identifie de manière unique le message R1. La valeur de la paire libellé-valeur 4213A permet à l'ordinateur 100 du serveur, lors de la réception du message R1, (1) d'envoyer un message de réponse associé R2 qu'on décrit ultérieurement, et (2) de déterminer si le message R1 est un message dupliqué (c'est-à-dire déjà reçu par l'ordinateur 100 du serveur). La valeur associée à la paire libellé-valeur 4213A est stockée dans le champ 251B de l'enregistrement 251 d'information sur l'inscription en attente de l'état civil/mise à jour de l'état civil (figure 5G).

La paire libellé-valeur 4213B comporte le libellé "date". La valeur de la paire libellé-valeur 4213B indique la date et l'heure auxquelles le message

R1 a été assemblé et envoyé à l'ordinateur 100 du serveur, selon l'horloge de l'ordinateur 200 du client. La valeur associée à la paire libellé-valeur 4213B est stockée dans le champ 251C.

La paire libellé-valeur 4213C comporte le libellé "code du serveur". Comme on le décrit ci-dessous, une paire code DES/VI utilisée par l'ordinateur 200 du client pour chiffrer la paire libellé-valeur opaque 4217 du message R1 est chiffrée en utilisant un code public RSA de l'ordinateur 100 du serveur. La valeur de la paire libellé-valeur 4213C est orientée vers le code privé RSA correspondant dans la structure 160 des données du code privé du serveur (figure 4A).

La paire libellé-valeur 4213D comporte le libellé "catégorie de service". La valeur de la paire 4213D est un libellé qui peut être utilisé pour acheminer le message R1 vers un processeur à l'intérieur de l'ordinateur 100 du serveur qui traite les messages d'une catégorie de service particulière. Cette option permet de répartir les fonctions de l'ordinateur 100 du serveur parmi les multiples processeurs, d'où l'amélioration de la capacité du système.

A l'étape 802C, le logiciel d'application 210 du client utilise des techniques bien connues pour produire une quantité aléatoire de 128 bits. On préfère que les 64 premiers bits de la quantité ainsi produite soient traités comme code DES de 56 bits et que les 64 seconds bits soient traités comme un vecteur d'initialisation de 64 bits ("VI"). Le code DES de 56 bits est représenté par une quantité de 64 bits ayant le bit de poids faible de chaque octet ignoré. Cette quantité de 128 bits peut être considérée comme une paire code DES/VI. La paire code DES/VI est stockée dans un registre temporaire.

Ensuite, à l'étape 804, le logiciel d'application 210 du client récupère le code public RSA pour l'ordinateur 100 du serveur à partir du champ 215A de la structure 215 des données d'application du client

(figure 5B). Comme on l'a indiqué précédemment, le code public RSA pour l'ordinateur 100 du serveur a de préférence 768 bits de long. Naturellement, on peut utiliser des codes RSA d'un autre longueur. A l'étape 806, le code public RSA récupéré à l'étape 804 est utilisé pour chiffrer la paire code DES/VI créée à l'étape 802.

A l'étape 807, le logiciel 210 accède à la structure 270 des données de la grille de messages (figure 2B) pour obtenir une liste de libellés, qui, lorsqu'ils sont adaptés à des valeurs associées, constituent les contenus de la section opaque du message R1, représenté en figure 10B. A l'étape 808, des valeurs sont associées à chaque libellé de la façon suivante :

La paire libellé-valeur 4217A comporte le libellé "type". La valeur de la paire libellé-valeur 4217A se rapporte à un enregistrement dans la structure 270 des données de message (figure 2B) qui établit les libellés du message R1. La valeur de la paire libellé-valeur 4217A est obtenue dans le logiciel d'application 210 du client qui produit le libellé lorsque l'utilisateur client 203 amorce l'opération d'inscription.

La paire libellé-valeur 4217B comporte le libellé "date de serveur". La valeur de la paire libellé-valeur 4217B indique la date et l'heure de l'assemblage du message R1 comme cela est mesurée par la perception par l'ordinateur 200 du client de la date de l'horloge de l'ordinateur 100 du serveur.

La paire libellé-valeur 4217C comporte le libellé "version du logiciel". La valeur de la paire libellé-valeur 4217C indique la version du logiciel d'application 210 du client qui communique avec l'ordinateur 100 du serveur. La valeur de la paire libellé-valeur 4217C est obtenue dans les données incorporées dans le logiciel d'application 210 du client. La valeur associée à la paire libellé-valeur 4217C est stockée dans le champ 251D.

La paire libellé-valeur 4217D comporte le libellé "contenu-langage". La valeur de la paire libellé-valeur 4217D indique un langage de communication préféré pour l'utilisateur client 203. La valeur de la paire 4217D est obtenue à partir de l'utilisateur 203 pendant l'opération d'inscription 401 à l'étape 1202. La valeur associée à la paire 4217D est stockée dans le champ 251E.

La paire libellé-valeur 4217E comporte le libellé "devise-implicite". La valeur de la paire 4217E indique une devise implicite dans laquelle les transactions de l'utilisateur client 203 seront traitées, sauf changement par cet utilisateur 203. La valeur de la paire 4217E est obtenue à partir de l'utilisateur 203 pendant l'opération d'inscription 401 à l'étape 1202 de la figure 8. La valeur associée à la paire libellé-valeur 4217E est stockée dans le champ 251F.

La paire libellé-valeur 4217F comporte le libellé "N° d'idendification demandé". La valeur de la paire 4217F indique le numéro d'identification d'état civil demandé par l'utilisateur client 203. La valeur de la paire 4217E est obtenue à partir de l'utilisateur 203 pendant l'opération d'inscription 401 à l'étape 1202 de la figure 8. La valeur associée à la paire libellé-valeur 4217F est stockée dans le champ 251G.

La paire libellé-valeur 4217G comporte le libellé "protocole de transport de courrier". La valeur de la paire 4217G indique une adresse de protocole de transport du courrier pour l'utilisateur client 203. La valeur de la paire 4217G est obtenue à partir de l'utilisateur 203 pendant l'opération d'inscription 401 à l'étape 1202 de la figure 8. La valeur associée à la paire libellé-valeur 4217G est stockée dans le champ 251H.

La paire libellé-valeur 4217H comporte le libellé "accords". La valeur de la paire 4217H indique les accords légaux que l'utilisateur client 203 a

acceptés dans le but d'utiliser la présente invention. Les accords légaux sont présentés à l'utilisateur 203 à l'étape 1202 de la figure 8. La valeur de la paire 4217H est produite lorsqu'un accord est accepté par l'utilisateur 203 et est stocké dans le champ 220L de la structure 220 des données de l'état civil de l'instrument financier du client (figure 5C).

La paire libellé-valeur 4217I comporte le libellé "autofermeture-phrase de passe". La valeur de la paire 4217I indique une phase de passe pour auto-fermeture pour le client utilisateur 203. La valeur de la paire 4217I est fournie par l'utilisateur 203 pendant l'opération d'inscription 401 à l'étape 1202 de la figure 8. La valeur associée à la paire 4217I est stockée dans le champ 220D de la structure 220 des données d'état civil du client et dans le champ 251I de la structure 250 des données en attente du client.

La paire libellé-valeur 4217J comporte le libellé "code public". La valeur de la paire 4217J représente le code public RSA pour l'état civil 120.1 du client produit par le logiciel d'application 210 du client pendant l'opération d'inscription 401 à l'étape 1202A de la figure 8.

De nouveau en liaison avec la figure 9, à l'étape 810, la signature numérique pour le message R1, représentée par la paire libellé-valeur 4217K de la figure 10B, est créée. La paire 4217K comporte le libellé "signature". La valeur de la paire 4217K représente la signature numérique de l'état civil 120.1 du client. Pour le message R1, la valeur de la paire 4217K est un contrôle de total de somme des caractères américains ASCII imprimables dans les paires libellé-valeur 4213A-4213C, et les paires libellé-valeur 4217A-4217J dans l'ordre alphabétique, chiffrées avec le code privé RSA de l'état civil 120.1. Le code privé RSA de l'état civil 120.1 est obtenu à partir du champ 220H (figure 5C).

A l'étape 812A, la paire libellé-valeur 4217K, créée dans l'étape 810, est annexée aux paires libellé-valeur 4217A-4217J. Les paires libellé-valeur 4217A-4217K sont chiffrées avec la paire codes DES/VI stockée dans le registre temporaire à l'étape 802C. A l'étape 812B, le résultat de l'étape 812A est annexé à la paire code DES chiffré RSA/VI qui a été créée dans l'étape 806.

A l'étape 813, la donnée assemblée à l'étape 812B est codée en utilisant des techniques bien connues (de préférence à base-64), complétant l'assemblage du contenu de la section opaque du message R1.

Le message R1 est assemblé aux étapes 814-818. A l'étape 814, l'en-tête 4205 est créé en utilisant la grille de messages trouvée dans la structure 270 des données de grille de messages du client (figure 5A) et un numéro de protocole inclus dans le logiciel d'application 210 du client.

Alors, à l'étape 815, des paires libellé-valeur transparentes 4213A-4213C telles que décrites ci-dessus sont ajoutées.

A l'étape 816, la paire libellé-valeur opaque 4217 est annexée. La paire 4217 comporte le libellé "opaque", signifiant que la valeur qui suit est une donnée chiffrée. La valeur de la paire 4217, représentée en figure 10A, représente la donnée qui a été codée à l'étape 813.

La queue 4250 est assemblée à l'étape 817. Le total de contrôle de la queue 4250 est calculé comme on l'a décrit ci-dessus en ce qui concerne le message échantillon 4000. La queue 4250 est ajoutée au message R1. A l'étape 818, une copie du message R1 est sauvegardée dans le champ 251J.

L'assemblage du message R1 est maintenant achevé. L'opération 800 d'assemblage de message se termine à l'étape 819.

De nouveau en liaison avec la figure 8, l'opération d'inscription 400 se poursuit à l'étape

1204. Là, l'ordinateur 200 du client transmet le message R1 à l'ordinateur 100 du serveur. L'ordinateur 200 attend un message de réponse R2 en provenance de l'ordinateur 100.

A l'étape 1205, l'ordinateur 100 reçoit le message R1 en provenance de l'ordinateur 200 du client et dévoile le message R1 en exécutant l'opération 900 de dévoilement de message du serveur. L'opération 900 sera maintenant décrite en liaison avec les figures 11A et 11B, où elle commence à l'étape 901.

A l'étape 901A, une copie du message R1 est stockée dans le champ 140E (figure 4L).

A l'étape 902, le logiciel 110 du serveur extrait le numéro de protocole dans le champ 4205C de l'en-tête 4205 du message R1. Ensuite, sur la base du numéro de protocole extrait à l'étape 902, la structure 150 des données de message du serveur (figure 4A) est accédée pour déterminer le format attendu du message R1. Le format attendu peut comprendre la syntaxe de message (par exemple, caractères de fin de ligne permis) et le code du message (par exemple ASCII ou hex). Le message R1 est analysé en conformité avec le format attendu de la manière suivante.

A l'étape 903, l'ordinateur 100 du serveur calcule un total de contrôle en utilisant la même donnée qui est employée par l'ordinateur 200 du client à l'étape 817 de l'opération 800 d'assemblage de message. A l'étape 904, le total de contrôle calculé à l'étape 903 est comparé au total de contrôle 4250D de la queue 4250 du message R1. Si les totaux de contrôle ne sont pas égaux, le message R1 est écarté à l'étape 904A où l'opération 900 de dévoilement de message du serveur se termine aussi.

Si les totaux de contrôle sont égaux à l'étape 904, le traitement se poursuit à l'étape 906A dans laquelle le message est vérifié pour déterminer s'il est approprié pour l'opération 900. Si un message comporte un libellé "code serveur", l'opération 900 est

appropriée. Les messages reçus par l'ordinateur 100 du serveur pour lesquels l'opération 900 est appropriée ne contiendront pas le libellé "code serveur" mais au contraire comprendront un libellé "type" dans la partie transparente du message. De tels messages seront dévoilés en utilisant d'autres modes opératoires qu'on décrit ultérieurement. Si un message est inapproprié, le traitement se poursuit à l'étape 906B dans laquelle le message est dirigé vers un autre mode opératoire de dévoilement. Le message R1 est approprié; par conséquent, le traitement se poursuit à l'étape 906C dans laquelle la valeur de la paire libellé-valeur opaque 4217 est décodée

A l'étape 907, le code public RSA utilisé par l'ordinateur 200 du client pour chiffrer la paire code DES/VI à l'étape 806 du mode opératoire 800 de l'assemblage du message est déterminé. Pour cela, le logiciel 110 du serveur obtient la valeur de la paire libellé-valeur 4213C associée au libellé "code serveur". La valeur de la paire 4213C est un pointeur dirigé vers un champ de la structure 160 des données de code privé qui stocke le composant code privé RSA qui correspond au code public RSA utilisé par l'ordinateur 200 du client à l'étape 806.

A l'étape 909, le code privé RSA déterminé à l'étape 907 est utilisé pour décrypter la partie de la paire libellé-valeur opaque 4217 qui correspond à la paire code DES chiffré par RSA/VI. De cette manière, la paire DES/VI utilisée pour chiffrer le reste de la paire libellé-valeur opaque 4217 est obtenue. A l'étape 909A, il y a détermination du fait que le chiffrement de la paire code DES/VI a réussi ou a échoué. Dans le cas où le décryptage a échoué pour une raison quelconque, le traitement se poursuit à l'étape 905 dans laquelle on trouve qu'il est préférable d'établir un indicateur d'erreur approprié et l'opération 900 de dévoilement du serveur se termine à l'étape 917. Si le décryptage de la

paire code DES/VI est réussi, le traitement se poursuit à l'étape 910.

A l'étape 910, la paire code DES/VI obtenue à l'étape 909 est stockée dans un registre temporaire.

A l'étape 911, la paire code DES/VI obtenue à l'étape 909 est utilisée pour décrypter la partie de la paire libellé-valeur opaque 4217 révélant les paires libellé-valeur 4217A-4217K de la figure 10B. A l'étape 912, il y a détermination du fait que le décryptage de la paire 4217 a réussi ou a échoué. Dans le cas où le décryptage a échoué pour une raison quelconque, le traitement se poursuit à l'étape 905 dans laquelle on trouve qu'il est préférable d'établir un indicateur d'erreur approprié et l'opération 900 du dévoilement du serveur se termine à l'étape 917. Si le décryptage de la paire 4217 est réussi, le traitement se poursuit à l'étape 913.

A l'étape 913, le type de message est déterminé par référence à la paire libellé-valeur 4217A. Par exemple, la valeur de la paire 4217A pour le message R1 peut être "inscription".

On a trouvé qu'il est préférable d'avoir trois contrôles du message R1 exécutés aux étapes 914, 915 et 916 de la façon suivante.

Le contrôle de forme du serveur de l'étape 914 est un type de message et dépend de la version du logiciel. Plus précisément, la forme attendue du message, et les critères qui déterminent s'il est acceptable, dépendent du message et de toute variation du message qui est valable à un instant donné comme cela est déterminé par référence à la structure 150 des données sur le type de message et sa version comme on l'a décrit précédemment. Comme minimum, le mode opératoire de contrôle de forme déterminera si un message entrant contient tous les libellés qui sont prescrits pour ce message, s'il y a ou non des valeurs pour chaque libellé qui nécessitent une valeur, et si les valeurs concernent le type, la syntaxe et la gamme

de valeurs selon nécessité. Si un message peut être analysé mais ne satisfait pas les critères de forme, l'ordinateur 100 du serveur établira un indicateur d'erreur à l'étape 905 et renverra un code d'erreur dans le message R2 (qu'on décrit ultérieurement). Un message qui est tellement mal formé qu'il ne peut être analysé par l'ordinateur 100 du serveur sera écarté. Si le contrôle de forme à l'étape 914 est réussi, le traitement se poursuit à l'étape 915.

A l'étape 915, la signature numérique représentée par la valeur de la paire libellé-valeur 4217K est vérifiée. Tout d'abord, le logiciel 110 du serveur obtient le code public RSA pour l'état civil 120.1 du client à partir de la valeur de la paire 4217J. Le code public RSA obtenu à partir de la paire 4217J est utilisé pour décrypter la paire 4217K. Ensuite, le logiciel 110 du serveur accède à la structure 150 des données de message afin de déterminer les paires libellé-valeur qui ont été l'objet d'un contrôle de total de somme à l'étape 810 de l'opération 800 d'assemblage de message afin de calculer la valeur de la paire 4217K. Le logiciel 110 procède alors à un contrôle de total de somme des mêmes paires libellé-valeur qui ont fait l'objet de ce contrôle à l'étape 810. Les deux valeurs des contrôles sont alors comparées. Si les valeurs sont différentes, un indicateur d'erreur approprié est établi à l'étape 905. Dans ce cas, l'opération 900 de dévoilement de message du serveur se termine à l'étape 917. Si les valeurs du contrôle de total de somme correspondent, le traitement se poursuit à l'étape 916.

A l'étape 916, un contrôle concernant le fait que le logiciel d'application 210 du client est courant est effectué de la façon suivante. Le logiciel 110 du serveur obtient le numéro de la version du logiciel d'application 210 du client qui est utilisé pour assembler le message R1 à partir de la valeur de la paire libellé-valeur 4217C. La valeur obtenue est

comparée au dernier numéro de version du logiciel d'application 210.

A chaque version est associé l'un de trois libellés "état". Si le contrôle du logiciel renvoie "courant", le logiciel d'application 210 du client qui a construit le message R1 est alors la dernière version disponible de ce logiciel. Aucun indicateur n'est établi et l'opération 900 de dévoilement de message se termine à l'étape 917. Si le contrôle du logiciel renvoie "avertissement", la version du logiciel 210 n'est pas la dernière, mais reste considérée comme utilisable. Un indicateur est établi à l'étape 905 qui aura pour effet qu'un message d'avertissement sera envoyé à l'utilisateur client 203 dans un message R2 (qu'on décrit ci-dessous) et l'opération 900 de dévoilement de message se termine à l'étape 917. Si le libellé associé au logiciel d'application 210 du client est "fatal", le logiciel n'est pas utilisable et un indicateur d'erreur est établi à l'étape 905 qui aura pour effet qu'un message d'erreur sera envoyé à l'utilisateur 203 dans le message R2 (qu'on décrit ci-dessous). L'opération 900 de dévoilement de message se termine à l'étape 917.

De nouveau en liaison avec la figure 8, le traitement se poursuit à l'étape 1206. Si l'un quelconque des tests des étapes 909A, 912, 914, 915 ou 916 a pour effet qu'un indicateur d'erreur est établi à l'étape 905, les opérations de traitement des erreurs seront exécutées par l'ordinateur 100 du serveur à l'étape 1215. Alors que le niveau du traitement d'erreur à l'étape 1215 est largement une décision administrative, on préfère qu'au minimum, les échecs du total de contrôle, de la signature, de la forme, et un retour "fatal" de l'opération de contrôle du logiciel se traduisent par un message de retour contenant un code qui peut être traité par le logiciel d'application 210 du client et par un message qui peut être lu par l'utilisateur client 203. L'opération de traitement des erreurs de l'étape 1215 implique l'association d'un

indicateur avec un code d'erreur spécifique (décrit ultérieurement dans le contexte du message de retour R2) et la création d'un message en texte (soit à partir d'une structure de données de message, soit d'un message envoyé par l'administrateur du système). L'ordinateur 100 du serveur produit alors un message R2 similaire à celui qu'on décrit ultérieurement pour l'ordinateur 200 du client qui achemine le code d'erreur et tout message concerné.

Si les tests des étapes 909A, 912, 914, 915 et 916 ne provoquent pas l'établissement d'un indicateur d'erreur à l'étape 915, le traitement se poursuit à l'étape 1207 dans laquelle la valeur de la paire libellé-valeur 4217F est comparée au numéro d'identification d'état civil du champ 120A pour tous les états civils 120.1 des clients et au champ 120AA pour tous les états civils 120.2 des commerçants qui sont contenus dans la structure 120 des données d'état civil du serveur.

A l'étape 1209, s'il est unique, le logiciel 110 du serveur crée un nouvel état civil 120.1 dans la structure 120 des données d'état civil du serveur. Une information contenue dans le message R1 est alors transférée au nouvel état civil 120.1 de la façon suivante : la valeur de la paire libellé-valeur 4217F, et le code de contrôle à deux chiffres, sont affectés au numéro d'identification d'état civil du champ 120A. La valeur de la paire libellé-valeur 4217G est stockée dans le champ 120B de l'adresse du protocole de transport de courrier. Le code public RSA du champ 120C reçoit la valeur de la paire libellé-valeur 4217J. La valeur de la paire libellé-valeur 4217B est affectée au champ 120D. La valeur de la paire libellé-valeur 4217D est stockée dans le champ 120E. La valeur de la paire libellé-valeur 4217H est stockée dans le champ 120I. La valeur de la paire libellé-valeur 4217I est stockée dans le champ 120F. Dans ce cas, le traitement se poursuit à l'étape 1217.

Ici, la valeur de la paire libellé-valeur 4217F n'est pas unique pour la structure 120 des données d'état civil du serveur à l'étape 1207, le traitement se poursuit à l'étape 1216.

A l'étape 1216, un numéro d'identification d'état civil suggéré est déterminé en calculant un nombre aléatoire et en l'annexant au numéro d'identification requis sans hyphénation. Ainsi "Brian" devient "Brian 15". Dans ce cas, le traitement se poursuit à l'étape 1217.

A l'étape 1217, le logiciel 110 du serveur assemble le message de réponse R2, représenté en figure 13, conformément à l'organigramme de la figure 12. La figure 12 décrit l'opération 1000 de l'assemblage d'un message du serveur.

L'opération 1000 de l'assemblage d'un message du serveur commence à l'étape 1001. Les étapes 1002A-1002B créent une paire libellé-valeur transparente 4313 du message R2. Les étapes 1002-1009 créent une paire libellé-valeur opaque 4317 du message R2. Les étapes 1010-1014 assemblent l'en-tête 4305, les paires libellé-valeur transparentes 4313A-4313C, la paire libellé-valeur opaque 4317 et la queue 4350 du message R2.

A l'étape 1002, le logiciel 110 du serveur accède à la structure 150 des donnéess de message (figure 4A) pour obtenir une liste de libellés, qui, lorsqu'ils correspondent aux valeurs associées, constituent les paires libellé-valeur transparentes 4313A-4313B du message R2. A l'étape 1002B, des valeurs sont associées à chaque libellé de la façon suivante :

La paire libellé-valeur 4313A comporte le libellé "transaction". La valeur de la paire 4313A est un numéro de transaction. La valeur de la paire 4313A est la même que celle reçue dans le message R1 dans la paire libellé-valeur 4213A.

Le champ 4313B comporte le libellé "date". La valeur de la paire 4313B est la même que celle reçue dans le message R1 dans la paire libellé-valeur 4213B.

La paire libellé-valeur 4313C comporte le libellé "catégorie de service". La valeur de la paire 4313C est la même que celle reçue dans le message R1 dans la paire libellé-valeur 4213D.

A l'étape 1002, le logiciel 110 du serveur accède à la structure 150 des données de la grille de messages pour obtenir une liste des libellés qui, lorsqu'ils correspondent aux valeurs associées, constituent le contenu de la section opaque du message R2, comme représenté en figure 13B.

Le traitement se poursuit à l'étape 1005. Là, les valeurs sont adaptées aux libellés pour former les paires libellé-valeur 4317A-4317K de la figure 13B.

Les contenus de la section opaque du message R2 sont représentés en figure 13B dans laquelle la paire libellé-valeur 4317A comporte le libellé "type". La paire 4317A se réfère à un enregistrement dans la structure 150 des données de message qui établit les libellés des contenus de la section opaque du message R2. La valeur de la paire 4317A est obtenue à partir du logiciel 110 du serveur.

La paire libellé-valeur 4317B comporte le libellé "serveur-date". La valeur de la paire 4317B indique la date et l'heure de l'assemblage du message R2 conformément à l'horloge de l'ordinateur 100 du serveur.

La paire libellé-valeur 4317C comporte le libellé "numéro d'identification requis". La valeur de la paire 4317C comporte le numéro d'identification d'état civil demandé par l'utilisateur client 203. La valeur de la paire 4317C est reçue dans la paire libellé-valeur 4217F du message R1.

La paire libellé-valeur 4317D comporte le libellé "numéro d'identification de réponse". La valeur de la paire 4317D indique le numéro d'identification de l'état civil de l'utilisateur client 203, ou, si le

numéro d'identification demandé dans la paire 4317C est une duplication, indique un numéro d'identification suggéré d'état civil.

La paire libellé-valeur 4317E comporte le libellé "protocole de transport de courrier". La valeur de la paire 4317E indique une adresse du protocole pour l'utilisateur client 203. La valeur de la paire 4317E est reçue dans la paire libellé-valeur 4217G du message R1.

La paire libellé-valeur 4317F comporte le libellé "code de réponse". La valeur de la paire 4317F indique si l'opération d'inscription 401 a été un succès ou un échec.

La paire libellé-valeur 4317G comporte le libellé "attente de fonds". La valeur de la paire 4317F indique s'il y a des messages comportant des fonds en attente pour le détenteur de l'adresse du protocole de transport de courrier dans la paire libellé-valeur 4317E. En variante, la paire pourrait indiquer le nombre de messages de cette nature. Chaque approche fournit un moyen grâce auquel l'inscrivant obtient de tels fonds en envoyant de préférence à l'ordinateur 100 du serveur un message contenant un mot de passe fourni par l'expéditeur des fonds.

La paire libellé-valeur 4317H comporte le libellé "phrase de passe d'auto-fermeture". La paire 4217H indique un mot de passe d'auto-fermeture pour l'utilisateur client 203. La valeur de la paire 4317H a été reçue dans la paire libellé-valeur 4217I du message R1.

La paire libellé-valeur 4317I comporte le libellé "code public". La valeur de la paire 4317I représentée en figure 13B indique le code public RSA de l'état civil 120.1 du client qui est reçu dans la paire 4217J du message R1.

La paire libellé-valeur 4317J comporte le libellé "sévérité de logiciel". La valeur de la paire 4317J indique si le logiciel d'application 210 du client

a besoin d'être mis à jour, mais reste utilisable ("avertissement") ou s'il n'est plus utilisable ("fatal"). La valeur de la paire 4317J est nulle si le logiciel 210 est courant.

La paire libellé-valeur 4317K comporte le libellé "message de logiciel". La valeur de la paire 4317K indique des instructions sur ce que l'utilisateur client 203 doit faire dans le cas d'une sévérité du logiciel "fatal" ou "avertissement". La valeur de la paire 4317K n'est présente que si la valeur de la paire 4317J n'est pas nulle.

La paire libellé-valeur 4317L comporte le libellé "message". La valeur de la paire 4317L est un message au texte libre qui est associé à une condition d'erreur ou de succès renvoyée dans la paire 4317F et affichée pour l'utilisateur client 203.

De nouveau en liaison avec la figure 12, le traitement se poursuit à l'étape 1007. Là, les paires libellé-valeur 4317A-4317L de la figure 13B sont assemblées et chiffrées avec la paire code DES/VI décryptée à l'étape 910.

A l'étape 1009, les paires libellé-valeur 4317A-4317L chiffrées à l'étape 1007 sont codées en utilisant des techniques bien connues (de préférence à base-64).

Le message R2 est assemblé aux étapes 1010-1014. A l'étape 1010, l'en-tête 4305 est assemblé en utilisant la structure 150 des données de message et de type et le numéro de protocole provenant du message entrant R1.

Ensuite, à l'étape 1011, les paires libellé-valeur transparentes 4313A et 4313B décrites précédemment sont ajoutées.

A l'étape 1012, la paire libellé-valeur opaque 4317 est annexée. La paire 4317 comporte le libellé "opaque" signifiant que la valeur qui suit est une donnée cryptée. La valeur de la paire 4317 représente la donnée codée à l'étape 1009.

La queue 4350 est assemblée à l'étape 1013. Le total de contrôle de la queue 4350 est calculé comme on l'a décrit ci-dessus en ce qui concerne le message échantillon 4000. La queue 4350 est ajoutée au message R2. A l'étape 1014, une copie du message complet R2 est sauvegardée au champ 140F de la structure 140 des données du journal de messages du serveur.

L'assemblage du message R2 est maintenant terminé. L'opération 1000 d'assemblage de message se termine à l'étape 1015.

De nouveau en liaison avec la figure 8, à l'étape 1218, le message R2 est envoyé de l'ordinateur 100 du serveur à l'ordinateur 200 du client.

A l'étape 1219, l'ordinateur 200 du client reçoit le message R2 en provenance de l'ordinateur 100 du serveur et dévoile le message R2 en exécutant l'opération 1100 de dévoilement de message. L'opération 1100 est maintenant décrite en liaison avec la figure 14, où il commence à l'étape 1101.

A l'étape 1102, le logiciel 210 de l'ordinateur du client extrait le numéro de protocole dans l'en-tête 4305 du message R2. Ensuite, sur la base du numéro de protocole extrait à l'étape 1102, la structure 270 des données de grille de message (figure 5A) est accédée pour déterminer le format attendu du message R2. Le format attendu peut comprendre une syntaxe de message (par exemple, caractères de fin de ligne permis) et un codage de message (par exemple ASCII ou hex). Le message R2 est analysé en conformité avec le format attendu comme suit.

A l'étape 1103, l'ordinateur 200 du client calcule un total de contrôle en utilisant la même donnée que celle utilisée par l'ordinateur 100 du serveur à l'étape 1013 de l'opération 1000 d'assemblage de message du serveur. A l'étape 1104, le total de contrôle calculé à l'étape 1103 est comparé au total de contrôle de la queue 4350 du message R2. Si les totaux de contrôle ne sont pas égaux, le message R2 est écarté à l'étape 1104A

dans laquelle l'opération 1100 de dévoilement de message se termine.

Si les totaux de contrôle sont égaux à l'étape 1104, le traitement se poursuit à l'étape 1105A dans laquelle le message est vérifié pour déterminer s'il est approprié pour l'opération 1100 de dévoilement de message. Si un message n'inclut pas le libellé "type" dans sa partie transparente, l'opération 1100 est inappropriée. Les messages reçus par l'ordinateur 200 du client contenant le libellé "type" dans leur partie transparente seront dévoilés en utilisant d'autres modes opératoires (décrits ailleurs) à l'étape 1105B. Ici, le message R2 est approprié; par conséquent, le traitement se poursuit à l'étape 1106C dans laquelle la valeur de la paire libellé-valeur opaque 4317 est décodée.

A l'étape 1107, la paire code DES/VI stockée dans le registre temporaire à l'étape 802 de l'opération 800 d'assemblage de message est récupérée.

A l'étape 1108, la paire code DES/VI récupérée à l'étape 1107 est utilisée pour décrypter la valeur de la paire libellé-valeur opaque 4317. Si pour une raison quelconque le décryptage de la paire 4317 n'est pas réussi, l'étape 1109 dirige le traitement du message R2 vers l'étape 1105 dans laquelle un indicateur d'erreur est établi. Dans ce cas, le traitement de l'opération 1100 de dévoilement de message s'arrête à l'étape 1121. Si le décryptage de la paire 4317 est réussi, le traitement se poursuit à l'étape 1110.

A l'étape 1110, le type de message est déterminé par référence à la paire libellé-valeur 4317A. Par exemple, la valeur de la paire 4317A pour le message R2 peut être "réponse à annonce".

Un contrôle de message R2 est alors effectué à l'étape 1111 comme suit. La structure 270 des données de grille de message (figure 5A) contient une donnée concernant la forme des messages entrants. Au minimum, l'opération de contrôle de forme établira si un message entrant contient tous les libellés qui sont prescrits

pour ce message, s'il y a des valeurs pour chaque libellé qui nécessitent une valeur, et si les valeurs sont du type (par exemple texte, numéros à signe), syntaxe (par exemple sous la forme d'une adresse valable de protocole de transport de courrier) et dans les limites spécifiées selon nécessité. S'il y a des libellés additionnels, l'ordinateur 200 du client les ignorera. Si un message ne peut être analysé, ou s'il peut être analysé mais ne satisfait pas un critère de forme, un indicateur d'erreur sera établi à l'étape 1105.

Si le message passe le contrôle de forme à l'étape 1111, l'opération 1100 de dévoilement de message se termine à l'étape 1121.

De nouveau en liaison avec la figure 8, le traitement se poursuit à l'étape 1220. Là, on a trouvé qu'il est préférable de traiter les messages d'erreur de la façon suivante :

(1) Si un indicateur d'erreur est établi à l'étape 1105, l'indicateur sera détecté à l'étape 1220 et le traitement du message R2 se terminera à l'étape 1221. A partir de la perspective de l'utilisateur client 203, aucune autre action n'est prise en ce qui concerne le message R2. Dans le mode de réalisation préféré de la présente invention, on préfère inclure un mécanisme dans le logiciel d'application 210 du client afin de créer et envoyer un message à l'ordinateur 100 du serveur. Ce message inclut le message R2 tel qu'il a été reçu par l'ordinateur 200 du client et tout diagnostic de ce qui a provoqué l'échec du message. Aucune réponse à ce message n'est envoyée par l'ordinateur 100 du serveur à l'ordinateur 200 du client. Au contraire, l'information est utilisée pour établir s'il existe un problème dans le système et si des mesures appropriées de correction doivent être prises.

(2) Si aucun indicateur d'erreur n'est établi à l'étape 1105 mais qu'une erreur dans le message R1 a été détectée à l'étape 905 ou à l'étape 1216, le

traitement se poursuivra à l'étape 1222 dans laquelle le contenu de la paire libellé-valeur 4317F est contrôlé. Si la valeur de la paire 4317F est autre que "succès", les sous-programme de traitement d'erreur sont exécutés à l'étape 1223, amenant le logiciel d'application 210 du client à afficher le message contenu dans la paire 4317K associée au contenu de la paire 4317F et à interpréter la valeur de la paire 4317F et à prendre toute action qui peut être associée à cette valeur. En particulier, si le seul indicateur d'erreur a été détecté à l'étape 1216, indiquant que le numéro d'identification requis n'est pas unique, le numéro d'identification suggéré par l'ordinateur 100 du serveur et renvoyé dans la paire libellé-valeur 4317D est affiché et l'opération d'inscription est redémarrée à l'étape 1201; ou

(3) si le message R1 passe le contrôle à l'étape 905 et qu'aucun indicateur n'est établi à l'étape 1105 et que le numéro d'identification demandé par l'utilisateur client 203 est accepté par l'ordinateur 100 du serveur, le traitement se poursuit à l'étape 1224 dans laquelle le logiciel d'application 210 du client met à jour la base de données 202 du client comme suit : la valeur de la paire libellé-valeur 4317D et le code de contrôle à deux chiffres sont affectés au numéro d'identification d'état civil du client du champ 220A. La valeur de la paire libellé-valeur 4317E est stockée dans l'adresse du protocole de transport du courrier du champ 220B. Le code public RSA du champ 220C reçoit la valeur créée par le logiciel d'application 210 du client et est renvoyé dans la paire 4317I. De plus, l'enregistrement 261 de la structure 260 des données du journal du client est créé de la façon suivante : le numéro de transaction dans la paire libellé-valeur 4313A est stocké dans le champ 261B. La date de la paire 4317B est stockée dans le champ 261C. Le numéro d'identification requis dans la paire libellé-valeur 4317C est stocké dans le champ 261H. Le numéro d'identification de réponse provenant de la paire 4317D

est stocké dans le champ 261I. L'adresse du protocole de transport de courrier dans la paire 4317E est stockée dans le champ 261J. Le code de réponse de la paire 4317F est stocké dans le champ 261F. Le code de sévérité du logiciel de la paire 4317J est stocké dans le champ 261D. Le message de logiciel de la paire 4317K est stocké dans le champ 261E. Le message de réponse associé au code de réponse du champ 4317L est stocké dans le champ 261G.

Le traitement se poursuit à l'étape 1225 dans laquelle l'opération d'inscription 401 se termine.

C. Opération de lien à un instrument financier 403.

L'opération 403 est une opération dans laquelle un utilisateur client 203 lie un instrument financier à un état civil 120.1 de client. La figure 15 décrit un organigramme illustrant le processus 403 de lien à un instrument qui commence à l'étape 1301.

A l'étape 1302, le logiciel d'application 210 du client indique à l'utilisateur client 203 d'entrer une information relative à un instrument financier devant être lié à l'état civil 120.1 du client. Cette information sera incluse dans le message BI1 envoyé à l'ordinateur 100 du serveur et fera partie de la donnée de lien à un instrument 120H (champs 120H.1-120H.28) pour l'instrument financier qui est lié. Dans le mode de réalisation préféré, l'utilisateur client 203 entre le numéro de l'instrument, la date d'expiration de l'instrument, le numéro d'identification du client de l'instrument, et le nom, l'adresse dans la rue, la ville, l'état, le code postal, le pays, le code de pays, et le numéro de téléphone (dont le code de la zone) du détenteur de l'instrument. Il sera également demandé à l'utilisateur client 203 d'indiquer si l'instrument qui est lié est l'instrument d'auto-fermeture comme on l'a décrit précédemment. De plus, le logiciel d'application 210 du client créera un nombre

aléatoire (désigné par "sel de l'instrument"). Il sera également demandé à l'utilisateur 203 une description de l'instrument qui est lié. Cette description peut être sous la forme de "carte de crédit de société" ou "compte bancaire de John". Pour les liens de cartes de crédit, cette information est stockée dans le champ 252R dans la structure 250 des données des transactions en attente du client. Le type d'instrument, la catégorie d'instrument, et les fonctions de l'instrument sont dérivés par le logiciel d'application 210 du client à partir de la donnée entrée par l'utilisateur client 203.

Alors que la donnée acquise à l'étape 1302 est décrite en liaison avec un instrument financier constitué d'une carte de crédit, il reste dans la connaissance du technicien de modifier la donnée de la carte de crédit pour tenir compte des cartes de débit, des CDA, et autres instruments financiers.

Le message BI1 sera assemblé par et transmis à partir de l'ordinateur 200 du client à l'ordinateur 100 du serveur pour effectuer l'opération 403 de lien à un instrument. On décrira maintenant les contenus du message BI1 en liaison avec les figures 16A et 16B.

La paire libellé-valeur 4413A comporte le libellé "numéro d'identification". La valeur de la paire 4413A indique le numéro d'identification de l'état civil pour l'utilisateur client 203. La valeur de la paire 4413A est obtenue à partir du champ 220A de la structure 220 des données d'état civil du client (figure 5B).

La paire libellé-valeur 4413B comporte le libellé "transaction". La valeur de la paire 4413B est un numéro de transaction, produit par le logiciel d'application 210 du client, qui identifie de manière unique le message BI1. La valeur associée à la paire 4413B est stockée dans le champ 252B (figure 5H).

La paire libellé-valeur 4413C comporte le libellé "date". La valeur de la paire 4413B indique la date et l'heure de l'assemblage du message BI1 et est envoyée à l'ordinateur 100 du serveur, conformément à

l'horloge de l'ordinateur 200 du client. La valeur associée à la paire 4413C est stockée dans le champ 252C de la structure 250 des données en attente du client.

La paire libellé-valeur 4413D comporte le libellé" code serveur". Comme on le décrit plus tard, la paire code DES/VI utilisée par l'ordinateur 200 du client pour crypter la paire libellé-valeur opaque 4417 du message BI1 est cryptée en utilisant un code public RSA de l'ordinateur 100 du serveur. La valeur de la paire 4413D est dirigée vers le code privé RSA correspondant qui est stocké dans la structure 160 des données de code privé du serveur.

La paire libellé-valeur 4413E comporte le libellé "catégorie de service". La valeur de la paire 4413 est un libellé qui peut être utilisé pour acheminer le message BI1 jusqu'à un processeur de l'ordinateur 100 du serveur qui traite les messages d'une catégorie de service particulière.

La paire libellé-valeur 4417 comporte le libellé "opaque" signifiant que la donnée qui suit comprend les contenus de la section opaque chiffrée du message BI1.

Les contenus de la section opaque du message BI1, représentés en figure 16B, seront maintenant décrits.

La paire libellé-valeur 4417A comporte le libellé "type". La valeur de la paire 4417A se rapporte à un enregistrement dans la structure 270 des données de message (figure 5A) qui établit les libellés des contenus de la section opaque du message BI1. La valeur de la paire 4417A est obtenue à partir du logiciel d'application 210 du client qui produit la valeur lorsque l'utilisateur client 203 amorce l'opération 403 de lien de l'instrument financier.

La paire libellé-valeur 4417B comporte le libellé "serveur-date". La paire 4417B indique la date et l'heure de l'assemblage du message BI1 telles qu'elles sont mesurées par la perception par

l'ordinateur 200 du client de l'horloge de l'ordinateur 100 du serveur.

La paire libellé-valeur 4417C comporte le libellé "version logiciel". La valeur de la paire 4417C indique la version du logiciel d'application 210 du client qui communique avec l'ordinateur 100 du serveur. La valeur de la paire 4417C est obtenue à partir de la donnée incorporée dans le logiciel d'application 210 du client. La valeur associée à la paire 4417C est stockée dans le champ 252D (figure 5H).

La paire libellé-valeur 4417D comporte le libellé "numéro d'instrument". Pour des raisons de sécurité, le numéro réel de l'instrument financier n'est pas stocké dans la base de données 102 de l'ordinateur 100 du serveur. Au contraire, le numéro est stocké dans la base de données 102 comme valeur de contrôle de total de somme. Le contrôle de total de somme de la valeur associée à la paire 4417D est stocké dans le champ 252F.

La paire libellé-valeur 4417E comporte le libellé "type d'instrument". La paire 4417E indique un type d'instrument, par exemple, VISA, MasterCard, American Express, etc. La valeur de la paire 4417E est obtenue à partir de l'utilisateur client 203 pendant l'opération 493 du lien de l'instrument financier à l'étape 1302 ou peut être dérivée par le logiciel d'application 210 du client à partir du numéro de l'instrument. La valeur associée à la paire 4417E est stockée dans le champ 252T.

La paire libellé-valeur 4417F comporte le libellé "catégorie d'instrument". La valeur de la paire 4417F indique la catégorie de l'instrument qui est lié. Les catégories peuvent comprendre, par exemple, des cartes de crédit, des cartes de débit, des CDA, etc. La valeur de la paire 4417F est dérivée par le logiciel d'application du client pendant l'opération 403 de lien de l'instrument à l'étape 1302.

La paire libellé-valeur 4417I comporte le libellé "fonctions d'instrument" et peut de préférence

avoir une combinaison quelconque des valeurs suivantes : "charge", "crédit", "chargement" ou "déchargment". La valeur de la paire 4417I indique une ou plusieurs fonctions qui peuvent être exécutées par l'utilisateur client 203 avec l'instrument qui est lié. Une transaction de charge se produit lorsqu'un état civil utilise un instrument lié comme une carte de crédit pour le paiement d'un produit. Une transaction de crédit est une opération dans laquelle un commerçant crédite l'état civil 120.1 du client au lieu de fournir le produit sur lequel ils se sont mis d'accord à l'origine. Les transactions de chargement et de déchargemeent sont les mêmes que celles décrites précédemment. La ou les fonctions de la paire 4417I sont dérivées par le logiciel 210 d'application du client pendant l'opération de lien de l'instrument à l'étape 1302.

La paire libellé-valeur 4417J comporte le libellé "sel d'instrument". La valeur de la paire 4417J indique un sel cryptographique utilisé pour réduire la facilité avec laquelle la valeur de la paire libellé-valeur 4417D (relative au numéro de l'instrument) peut être déterminée. La valeur de la paire 4417J est produite par le logiciel d'application 210 du client pendant l'opération 403 de lien de l'instrument à l'étape 1302. La valeur associée à la paire 4417J est stockée dans le champ 252U (figure 5H).

La paire libellé-valeur 4417K comporte le libellé "date d'expiration de l'instrument". La valeur de la paire 4417H indique la date d'expiration de l'instrument qui est lié. La valeur de la paire 4417K est obtenue auprès de l'utilisateur client 203 pendant l'opération 403 de lien de l'instrument à l'étape 1302. La valeur associée à la paire 4417K est stockée dans le champ 252I.

La paire libellé-valeur 4417L comporte le libellé "nom d'instrument". La valeur de la paire 4417L indique le nom du détenteur de l'instrument qui est lié. La valeur de la paire 4417L est obtenue auprès de

l'utilisateur client 203 pendant l'opération 403 de lien de l'instrument à l'étape 1302. La valeur associée avec la paire 4417L est stockée dans le champ 252H.

La paire libellé-valeur 4417M comporte le libellé "instrument-rue". La valeur de la paire 4417M indique l'adresse de la rue du détenteur de l'instrument qui est lié. La valeur de la paire 4417M est obtenue auprès de l'utilisateur client 203 pendant l'opération 403 de lien de l'instrument à l'étape 1302.

La paire libellé-valeur 4417N comporte le libellé "instrument-ville". La valeur de la paire 4417N indique la ville du détenteur de l'instrument qui est lié. La valeur de la paire 4417N est obtenue auprès de l'utilisateur client 203 pendant l'opération 403 de lien de l'instrument à l'étape 1302.

La paire libellé-valeur 4417O comporte le libellé "instrument-état". La valeur de la paire 4417O indique l'état du détenteur de l'instrument qui est lié. La valeur de la paire 4417O est obtenue auprès de l'utilisateur client 203 pendant l'opération 403 de lien de l'instrument à l'étape 1302.

La paire libellé-valeur 4417P comporte le libellé "instrument-code postal". La valeur de la paire 4417P indique le code postal du détenteur de l'instrument qui est lié. La valeur de la paire 4417P est obtenue auprès de l'utilisateur client 203 pendant l'opération 403 de lien de l'instrument à l'étape 1302.

La paire libellé-valeur 4417Q comporte le libellé "instrument-pays". La valeur de la paire 4417Q indique le pays du détenteur de l'instrument qui est lié. La valeur de la paire 4417Q est obtenue auprès de l'utilisateur client 203 pendant l'opération 403 de lien de l'instrument à l'étape 1302.

La valeur associé aux paires libellé-valeur 4417M-4417Q sont stockées dans les champs 252I-252N (figure 5H).

La paire libellé-valeur 4417R comporte le libellé "accords". La valeur de la paire 4417R indique

les accords légaux que l'utilisateur client 203 a acceptés dans le but d'utiliser la présente invention. La valeur de la paire 4417R est produite à partir de l'accord accepté par l'utilisateur client 203 et est stockée dans le champ 230S (figure 5D).

La paire libellé-valeur 4417S comporte le libellé "auto-fermeture" et peut avoir la valeur "oui" ou "non". La valeur de la paire 4417S indique si l'instrument qui est lié sera l'instrument à auto-fermeture pour l'utilisateur client 203. La valeur de la paire 4417S est obtenue auprès de l'utilisateur client 203 pendant l'opération 403 de lien de l'instrument à l'étape 1302.

La paire libellé-valeur 4417T comporte le libellé "auto-fermeture-phrase de passe". La valeur de la paire 4417T indique la phrase de passe (six à cinquante caractères) qui, lorsqu'elle est utilisée, fermera l'état civil 120.1 du client. La paire 4417T est seulement présente si sa valeur est "oui". La valeur de la paire 4417T est fournie par l'utilisateur client 203 pendant l'opération d'inscription 401.

La paire libellé-valeur 4417U comporte le libellé "code". La valeur de la paire 4417U représente un contrôle de total de somme de la partie modulus de la paire code public RSA/code privé pour l'état civil 120.1 du client. La valeur de la paire 4417U permet à l'ordinateur 100 du serveur de confirmer que le code public RSA maintenu dans le champ 120B (figure 4B) est le même code que celui utilisé pour signer le message BI1 (paire 4417V).

La signature numérique du message BI1, représentée par la paire libellé-valeur 4417V, comporte le libellé "signature". La valeur de la paire 4417V représente la signature numérique de l'état civil 120.1 du client. Pour le message BI1, la valeur de la paire 4417V est de préférence un contrôle total de somme des paires 4413A-4413D, et des paires 4417A-4417U dans l'ordre alphabétique, cryptée avec le code privé RSA de

l'état civil 120.1 du client. Le code privé RSA de l'état civil 120.1 est obtenu à partir du champ 220H (figure 5C).

De nouveau en liaison avec la figure 15, à l'étape 1303, le message BI1 est assemblé en conformité avec l'opération 800 d'assemblage de message, décrite en figure 9. L'opération 800 a été décrite précédemment pour l'assemblage du message d'inscription R1, avec la modification suivante notée pour le message BI1 : une copie du message BI1 est de préférence sauvegardée dans le champ 252W (figure 5H), l'opération 403 de lien de l'instrument se poursuit à l'étape 1304. Là, l'ordinateur 200 du client transmet un message BI1 à l'ordinateur 100 du serveur. L'ordinateur 200 du client attend le message de réponse BI4 en provenance de l'ordinateur 100 du serveur.

A l'étape 1305, l'ordinateur 100 du serveur reçoit le message BI1 en provenance de l'ordinateur 200 et dévoile le message BI1 en exécutant l'opération 900 de dévoilement de message du serveur (étapes 901-917). L'opération 900 (étapes 901-917) a été précédemment décrite en liaison avec la figure 11 pour le message R1.

A l'étape 1306, si l'un quelconque des tests des étapes 909A, 912, 914, 915 ou 916 a provoqué l'établissement d'un indicateur d'erreur à l'étape 905, des opérations de traitement des erreurs sont exécutées par l'ordinateur 100 du serveur à l'étape 1313.

Alors que le niveau du traitement des erreurs à l'étape 1313 est largement une décision administrative, on préfère qu'au minimum, les échecs du total de contrôle, de la signature, et de la forme, et un retour "fatal" sur l'opération de contrôle du logiciel se traduisent par un message de retour contenant un code qui peut être traité par le logiciel d'application 210 du client et par un message qui peut être lu par l'utilisateur client 203. L'opération de traitement des erreurs de l'étape 1313 implique l'association d'un indicateur à un code d'erreur

spécifique (décrit dans le contexte du message de retour BI4 ci-dessous) et la création d'un message de texte (soit à partir d'une structure de données de messages soit d'un message envoyé par l'administrateur du système). L'ordinateur 100 du serveur envoie alors un message BI4 similaire à celui décrit ultérieurement à l'ordinateur 200 du client, acheminant le code d'erreur et tout message concerné.

Si les tests des étapes 909A, 912, 904, 905 et 916 n'ont pas provoqué l'établissement d'un indicateur d'erreur à l'étape 905, le traitement se poursuit à l'étape 1307. Là, l'information contenue dans le message BI1 est transférée à la donnée du lien de l'instrument 120H (champs 120H.1-120H.28) (Figure 4D) de la façon suivante : la valeur de la paire libellé-valeur 4413A est stockée dans le numéro d'identification d'état civil du champ 120H.1. La valeur de la paire 4417A est stockée dans le type d'instrument du champ 120H.2. La valeur de la paire 4417B est stockée dans la date de lien de l'instrument du champ 120H.13. Si l'instrument qui est l'objet du lien est choisi par l'utilisateur client 203 comme l'instrument à auto-fermeture, la valeur de la paire 4417D est stockée dans le numéro d'instrument du champ 120H.4. On préfère que cette valeur soit cryptée en utilisant un code RSA connu seulement de l'opérateur du système. Si l'instrument qui est lié n'est pas un instrument à auto-fermeture d'état civil, la valeur de la paire 4417D n'est pas stockée dans la structure 102 des donnéess du serveur mais est l'objet d'un contrôle de total de somme en même temps que la valeur dans la paire 4417J et stockée dans le contrôle de total de somme d'instrument du champ 120H.9. La valeur de la paire 4417E est stockée dans le sous-type d'instrument du champ 120H.3. La valeur de la paire 4417F est stockée dans le type d'instrument du champ 120H.2. La valeur de la paire 4417R est stockée dans les accords légaux du champ 120H.7. La valeur de la paire

4417S est stockée dans le lien d'auto-fermeture du champ 120F.

Après l'étape 1307, le message BI4 sera assemblé par et transmis par l'ordinateur 100 du serveur à l'ordinateur 200 du client pour achever l'opération 403 de lien de l'instrument. Le contenu du message BI4 sera maintenant décrit en liaison avec les figures 17A et 17B.

La paire libellé-valeur 44.113A comporte le libellé "numéro d'identification". La valeur de la paire 44.113A indique le numéro d'identification d'état civil pour l'utilisateur client 203. La valeur de la paire 44.113A est la même que celle reçue dans le message BI1 dans la paire 4413A.

La paire libellé-valeur 44.113B comporte le libellé "transaction". La valeur de la paire 44.113B est un numéro de transaction. La valeur de la paire 44.113B est la même que celle reçue dans le message BI1 dans la paire 4413B.

Le champ 44.113C comporte le libellé "date". La valeur de la paire 44.113C est la même que celle reçue dans le message BI1 dans la paire 4413C.

La paire libellé-valeur 44.113D comporte le libellé "catégorie de service". La valeur de la paire 44.113D est la même que celle reçue dans le message BI1 dans la paire 4413E.

Le contenu de la section opaque du message BI4, représenté en figure 17B, sera maintenant décrit.

La paire libellé-valeur 44.117A comporte le libellé "type". La valeur de la paire 44.117A se rapporte à un enregistrement dans la structure 270 des données de message (figure 5A) qui établit les libellés du contenu de la section opaque du message BI4. La valeur de la paire 44.117A est obtenue auprès du logiciel 110 du serveur.

La paire libellé-valeur 44.117B comporte le libellé "serveur-date". La valeur de la paire 44.117B

indique la date et l'heure de l'assemblage du message BI14 selon l'horloge de l'ordinateur 100 du serveur.

La paire libellé-valeur 44.117C comporte le libellé "code de réponse" et de préférence la valeur "succès" ou "échec". La valeur de la paire 44.117C indique que si l'opération 403 de lien de l'instrument a été un succès ou un échec.

La paire libellé-valeur 44.117D comporte le libellé "sévérité du logiciel" et de préférence la valeur "fatal" ou "avertissement". La valeur de la paire 44.117D indique si le logiciel d'application 210 du client doit être mis à jour, mais reste utilisable ("avertissement") ou s'il n'est plus utilisable ("fatal"). La valeur de la paire 44.117D est nulle si le logiciel d'application 210 est courant.

La paire libellé-valeur 44.117E comporte le libellé "message de logiciel". La valeur de la paire 44.117E fournit les instructions sur ce que doit faire l'utilisateur client 203 en cas de la sévérité "fatal" ou "avertissement" du logiciel. La valeur de la paire 44.117E n'est présente que si la valeur de la paire 44.117D n'est pas nulle.

La paire libellé-valeur 44.117F comporte le libellé "numéro d'instrument". La valeur de la paire 44.117F indique le numéro de l'instrument qui est l'objet d'un lien comme on l'a décrit ci-dessus. La valeur de la paire 44.117F est obtenue à partir de la paire 4417D du message BI1.

La paire libellé-valeur 44.117G comporte le libellé "type d'instrument". La valeur de la paire 44.117G indique le type d'instrument. La valeur de la paire 44.117G est obtenue à partir de la paire 4417E du message BI1.

La paire libellé-valeur 44.117H comporte le libellé "sel d'instrument". La valeur de la paire 44.117H est obtenue à partir de la paire 4417J du message BI1.

La paire libellé-valeur 44.117J comporte le libellé "fonctions d'instrument" et peut avoir n'importe quelle combinaison des valeurs suivantes : "vente", "crédit", "chargement" ou "déchargement" comme on l'a décrit précédemment. La paire 44.117J indique une ou plusieurs fonctions qui peuvent être exécutées par l'utilisateur client 203 avec l'instrument qui est lié. La valeur de la paire 44.117J est obtenue à partir de la paire 4417I du message BI1.

La paire libellé-valeur 44.117K comporte le libellé "instrument*" et représente tout nombre de paires libellé-valeur dont les libellés commencent avec "instrument" qui sont fournis à l'utilisateur client 203 dans le message BI4 (comme décrit précédemment) et renvoyés à l'ordinateur 100 du serveur dans le message LU1 lorsque l'instrument est utilisé pour le chargement ou le déchargement de fonds. De cette façon, l'ordinateur 100 du serveur peut recevoir une information concernant l'instrument lorsque cela est nécessaire sans stocker cette information dans ses structures de données. Les paires donnée-valeur particulières qui sont contenues dans la paire libellé-valeur 44.117K dépendent du type de l'instrument lié et des exigences de l'émetteur de l'instrument financier. Par exemple, une carte de crédit pourrait nécessiter le numéro de carte, la date d'expiration de la carte, et le nom et l'adresse du détenteur de la carte pour être renvoyés au serveur chaque fois que la carte est utilisée pour charger des fonds dans l'état civil 120.1.

La paire libellé-valeur 44.117L comporte le libellé "message". La valeur de la paire 44.117L est un message en texte libre qui est associé à une condition d'erreur ou de succès renvoyée dans la paire 44.117C et affichée chez l'utilisateur client 203. La valeur de la paire 44.117L peut inclure un message indiquant une mauvaise signature numérique ou un message BI1 d'inscription et des instructions mal formées sur la

façon dont l'utilisateur client 203 doit procéder (par exemple "appeler l'administrateur du système").

De nouveau en liaison avec la figure 15, à l'étape 1308, le message BI4 est assemblé en conformité avec l'opération 1000 d'assemblage de message du serveur, décrit en figure 13. L'opération 1000 a été décrite antérieurement pour l'assemblage du message d'inscription R2.

A l'étape 1309, l'ordinateur 200 du client reçoit le message BI4 en provenance de l'ordinateur 100 du serveur et dévoile le message BI4 en exécutant l'opération 110 de dévoilement de message (étapes 1101-1121). L'opération 110 a été décrite précédemment en liaison avec la figure 14 pour le message R2.

A l'étape 1310,

(1) Si un indicateur d'erreur a été établi à l'étape 1105, l'indicateur sera détecté à l'étape 1310 et le traitement du message BI4 sera terminé à l'étape 1311. A partir de la perspective de l'utilisateur client 203, aucune autre action n'est prise en ce qui concerne le message BI4. Dans la présente invention, un mécanisme est fourni dans le logiciel d'application 210 du client pour créer et envoyer un message à l'ordinateur 100 du serveur. Ce message comprend le message BI4 tel qu'il est reçu par l'ordinateur 100 du client et tout diagnostic sur ce qui a provoqué l'échec du message. Aucune réponse à ce message n'est envoyée par l'ordinateur 100 du serveur à l'ordinateur 200 du client. Au contraire, l'information est utilisée pour indiquer s'il existe un problème dans le système et si des mesures correctives appropriées doivent être prises.

(2) Si aucun indicateur d'erreur n'a été établi dans l'étape 1105 mais qu'une erreur dans le message BI1 a été détectée à l'étape 905, le traitement se poursuivra à l'étape 1312 dans laquelle le contenu de la paire libellé-valeur 44.117C est vérifié. Si la valeur de la paire 44.117C est autre que "succès", les sous-programmes de traitement d'erreur sont exécutés à

l'étape 1314, amenant le logiciel d'application 210 du client à afficher le message contenu dans la paire 44.117L associée au contenu de la paire 44.117C et à interpréter la valeur de la paire 44.117C et prendre toute action qui peut être associée à cette valeur; ou

(3) si le message BI1 a passé la vérification à l'étape 905 et qu'aucun indicateur d'erreur n'a été établi à l'étape 1105, le traitement se poursuit à l'étape 1315 dans laquelle le logiciel d'application 210 du client met à jour la base de donnée 202 du client de la façon suivante : le numéro d'instrument provenant de la paire 44.117F est stocké dans le champ 230A (figure 5D). Le contenu de la paire 44.117J est utilisé pour établir des indicateurs dans les champs 230L-230O. Le code de résultat contenu dans la paire 44.117C est sauvegardé dans le champ 230P. Le contenu de la paire 44.117K est stocké dans le champ 230R. De plus, un nouvel enregistrement 262 (figure 5O) de la structure 260 des données du journal du client est créé de la façon suivante : le numéro de la transaction provenant de la paire 44.113B est stocké dans le champ 262B. La date de la paire 44.117B est stockée dans le champ 262C. Le code de réponse de la paire 44.117C est stocké dans le champ 262F. Le code de sévérité du logiciel de la paire 44.117D est stocké dans le champ 262D. Le message de logiciel de la paire 44.117E est stocké dans le champ 262E. Le numéro d'instrument de la paire 44.117F est stocké dans le champ 262I. Le type d'instrument de la paire 44.117G est stocké dans le champ 262J. Le message de réponse associé au code de réponse du champ 44.117L est stocké dans le champ 262G.

Le traitement se poursuit à l'étape 1315 dans laquelle l'opération 403 de lien de l'instrument se termine.

D. Opération 405 de chargement/déchargement de fonds.

La figure 18 décrit un organigramme illustrant une opération de chargement/déchargement 405 qui commence à l'étape 1401.

A l'étape 1401A, l'utilisateur client 203 choisit s'il décide de charger ou de décharger des fonds. Dans le but de la présente description, on suppose que l'utilisateur 203 décide de charger des fonds. Le déchargement des fonds suit le même processus sauf que les fonds devant être déchargés sont spécifiés comme quantité négative.

A l'étape 1402, le logiciel d'application 210 du client accède au champ 2300 de l'enregistrement 230.1 pour tous les instruments liés à l'état civil 120.1 et affiche une liste de tous les instruments validés pour des opérations de chargement. A l'étape 1403, l'utilisateur client 203 est avisé de sélectionner un instrument dans la liste affichée pour charger des fonds dans le conteneur d'espèces représenté par les champs des données du conteneur d'espèces 120G et 220I.

A l'étape 1406, l'utilisateur client 203 est avisé d'entrer le montant des fonds dans une devise spécifiée pour chargement à partir de l'instrument choisi à l'étape 1402 dans le conteneur d'espèces 120G.

Le message LU1 sera assemblé par et transmis de l'ordinateur 200 du client à l'ordinateur 100 du serveur pour effectuer l'opération 405 de chargement/déchargement de fonds. Le contenu du message LU1 est maintenant décrit en liaison avec les figures 19A et 19B.

La paire libellé-valeur 4513A comporte le libellé "numéro d'identification". La valeur de la paire 4513A indique le numéro d'identification de l'état civil pour l'utilisateur client 203. La valeur de la paire 4513A est obtenue à partir du champ 220A (figure 5C) La

valeur associée à la paire 4513A est stockée dans le champ 255E (figure 5K).

La paire libellé-valeur 4513B comporte le libellé "transaction". La valeur de la paire 4513B est un numéro de la transaction, produit par le logiciel d'application 210 du client, qui identifie de manière unique le message LU1. La valeur de la paire 4513B permet à l'ordinateur 100 du serveur, sur réception du message LU1, (1) d'envoyer un message associé de réponse LU2 qu'on décrit ultérieurement, et (2) de déterminer si le message LU1 est un message en double (c'est-à-dire déjà reçu par l'ordinateur 100 du serveur). La valeur associée à la paire 4513B est stockée dans le champ 255B.

La paire libellé-valeur 4513C comporte le libellé "date". La valeur de la paire 4513C indique la date et l'heure de l'assemblage du message LU1 et est envoyée à l'ordinateur 100 du serveur, conformément à l'horloge de l'ordinateur 200 du client. La valeur associée à la paire 4513C est stockée dans le champ 255E.

La paire libellé-valeur 4513D comporte le libellé" code serveur". Comme décrit ci-dessous, la paire code DES/VI utilisée par l'ordinateur 200 du client pour crypter la paire libellé-valeur opaque 4517 du message LU1 est cryptée en utilisant un code public RSA de l'ordinateur 100 du serveur. La valeur de la paire libellé-valeur 4513D est dirigée sur le code privé RSA correspondant qui est stocké dans la structure 160 des données de code privé du serveur.

La paire libellé-valeur 4513E comporte le libellé "catégorie de service". La valeur de la paire 4513E est un libellé qui peut être utilisé pour acheminer le message LU1 jusqu'à un processeur situé dans l'ordinateur 100 du serveur qui traite les messages d'une catégorie de service particulière.

La paire libellé-valeur 4517 comporte le libellé "opaque" signifiant que la donnée qui suit

comprend les contenus de la section opaque cryptée du message LU1. Les contenus de la section opaque du message LU1, représentés en figure 19B, seront maintenant décrits.

La paire libellé-valeur 4517A comporte le libellé "type". La valeur de la paire 4517A se rapporte à un enregistrement dans la structure 150 des données de message (figure 4A) qui établit les libellés des contenus de la section opaque du message LU1. La valeur de la paire 4517A est obtenue à partir du logiciel d'application 210 du client qui produit le libellé lorsque l'utilisateur client 203 amorce l'opération 405 de chargement/déchargement.

La paire libellé-valeur 4517B comporte le libellé "date de serveur". La paire 4517B indique la date et l'heure de l'assemblage du message LU1 telles qu'elles sont mesurées par la perception par l'ordinateur 200 du client de l'horloge de l'ordinateur 100 du serveur.

La paire libellé-valeur 4517C comporte le libellé "version logiciel". La valeur de la paire 4517C indique la version du logiciel d'application 210 du client qui communique avec l'ordinateur 100 du serveur. La valeur de la paire 4517C est obtenue à partir de la donnée incorporée dans le logiciel d'application 210 du client. La valeur associée à la paire 4517C est stockée dans le champ 255D (figure 5K).

La paire libellé-valeur 4517D comporte le libellé "montant". La valeur de la paire 4517D représente le type de devise et le montant des fonds à transférer à partir de l'instrument lié qui est sélectionné à l'étape 1402 vers le conteneur d'espèces 120G pour l'utilisateur client 203. Pour des opérations de déchargement, le montant des fonds est une quantité négative. Ainsi, pour des déchargements, la valeur de la paire 4517D représente le type de devise et le montant des fonds à transférer du conteneur 120G à l'instrument lié qui est sélectionné à l'étape 1402. La valeur

associée à la paire 4517D est stockée dans le champ 255G.

La paire libellé-valeur 4517E comporte le libellé "instrument*" et représente toutes les paires libellé-valeur renvoyées par l'ordinateur 100 du serveur dans le message BI4 dans la paire libellé-valeur 44.117K (figure 17A) dont le libellé commence par "instrument". La valeur de la paire 4517E est unique pour l'instrument à partir duquel l'opération de chargement doit être exécutée et identifie cet instrument pour l'ordinateur 100 du serveur.

La paire libellé-valeur 4517F comporte le libellé "code". La valeur de la paire 4517F représente un contrôle de total de somme de la partie modulus de la paire code public RSA/code privé utilisée par l'état civil 120.1 du client. La valeur de la paire 4517F permet à l'ordinateur 100 du serveur de confirmer que le code public RSA maintenu dans le champ 120B (figure 4B) est le même code que celui utilisé pour signer le message LU1 (paire libellé-valeur 4517F).

De nouveau en liaison avec la figure 18, à l'étape 1407, le message LU1 est assemblé en conformité avec l'opération 800 d'assemblage de message, (figure 9). L'opération 800 a été décrite précédemment pour l'assemblage du message d'inscription R1, avec la modification suivante notée pour le message LU1. Une copie du message LU1 est de préférence sauvegardée dans le champ 140E (figure 4L).

L'opération 405 de chargement/déchargement se poursuit à l'étape 1408. Là, l'ordinateur 200 du client transmet le message LU1 à l'ordinateur 100 du serveur. L'ordinateur 200 attend un message de réponse LU2 provenant de l'ordinateur 100.

A l'étape 1409, l'ordinateur 100 du serveur reçoit le message LU1 provenant de l'ordinateur 200 du client et dévoile le message LU1 en exécutant l'opération 900 de dévoilement de message du serveur (étapes 901-917). L'opération 900 a été décrite

précédemment en liaison avec la figure 11 pour le message R1.

De nouveau en liaison avec la figure 14, le traitement se poursuit à l'étape 1410, si l'un quelconque des tests des étapes 909A, 912, 914, 915 ou 916 a provoqué l'établissement d'un indicateur d'erreur à l'étape 905, les opérations de traitement des erreurs sont exécutées par l'ordinateur 100 du serveur à l'étape 1417. Alors que le niveau du traitement des erreurs à l'étape 1417 est largement une décision administrative, on préfère qu'au minimum, les échecs du total de contrôle, de la signature, et de la forme, et un retour "fatal" de l'opération de vérification du logiciel se traduisent par un message de retour contenant un code qui peut être traité par le logiciel d'application 210 du client et par un message qui peut être lu par l'utilisateur client 203. L'opération de traitement des erreurs dans l'étape 1418 implique l'association d'un indicateur avec un code d'erreur spécifique (qu'on décrit dans le contexte du message de retour LU2 ci-après) et la création d'un message en texte (soit à partir d'une structure de données de message soit d'un message envoyé par l'administrateur du système). L'ordinateur 100 du serveur produit alors un message LU2 semblable à celui décrit ci-dessous pour l'ordinateur 200 du client, acheminant le code d'erreur et tout message concerné.

Si les tests des étapes 909A, 912, 914, 915 et 916 n'ont pas provoqué l'établissement d'un indicateur d'erreur à l'étape 905, le traitement se poursuit à l'étape 1411. Là, l'information contenue dans le message LU1, c'est-à-dire le montant représenté par la paire libellé-valeur 4517D est ajoutée au montant du conteneur d'espèces du champ 120G.2 de l'état civil 120.1 pour l'utilisateur client 203 dans la structure 120 des données d'état civil du serveur. A ce point, l'ordinateur 100 du serveur provoquera le transfert des fonds de l'instrument indiqué dans le message LU1 au

compte de l'agence identifié dans le champ 120G.4 du conteneur d'espèces. Les fonds demandés dans le message LU1 peuvent être placés "en suspens" d'une manière telle qu'ils ne sont pas disponibles jusqu'à ce qu'une condition additionnelle soit satisfaite, par exemple jusqu'à ce qu'il y ait écoulement d'un laps de temps de vingt-quatre heures.

Après l'étape 1411, le message LU2 sera assemblé par et transmis à partir de l'ordinateur 100 du serveur à l'ordinateur 200 du client pour achever l'opération 405 de chargement/déchargement des fonds. On décrira maintenant le contenu du message LU2 en liaison avec les figures 20A et 20B.

La paire libellé-valeur 45.113A comporte le libellé "numéro d'identification". La valeur de la paire 45.113A indique le numéro d'identification d'état civil pour le client utilisateur 203. La valeur de la paire 45.113A est la même que celle reçue dans le message LU1 dans la paire 4513A.

La paire libellé-valeur 45.113B comporte le libellé "transaction". La valeur de la paire 45.113B est un numéro de transaction. La valeur de la paire 45.113B est la même que celle reçue dans le message LU1 dans la paire 4513B.

La paire libellé-valeur 45.113C comporte le libellé "date". La valeur de la paire 45.113C est la même que celle reçue dans le message LU1 dans la paire 4513C.

La paire libellé-valeur 45.113D comporte le libellé "catégorie de service". La valeur de la paire 45.113D est la même que celle reçue dans le message LU1 dans la paire 4513E.

Le contenu de la section opaque du message de réponse LU2, représenté en figure 20B, est le suivant :

La paire libellé-valeur 45.117A comporte le libellé "type". La valeur de la paire 45.117A concerne un enregistrement dans la structure 270 des données de

message (figure 5A) qui établit les libellés des contenus de la section opaque du message LU2. La valeur de la paire 45.117A est obtenue à partir du logiciel 110 du serveur.

La paire libellé-valeur 45.117B comporte le libellé "date de serveur". La valeur de la paire 45.117B indique la date et l'heure de l'assemblage du message LU2 conformément à l'horloge de l'ordinateur 100 du serveur.

La paire libellé-valeur 45.117C comporte le libellé "montant". La valeur de la paire 45.117C est le montant transféré à partir de l'instrument lié qui est identifié par la paire 4517E au champ 120G.2 du conteneur d'espèces pour l'utilisateur client 203.

La paire libellé-valeur 45.117D comporte le libellé "code de réponse" et la valeur "succès" ou "échec" comme on l'a décrit précédemment. La valeur de la paire 45.117D indique si l'opération 405 de chargement/déchargement a été un succès ou un échec.

La paire libellé-valeur 45.117E comporte le libellé "message". la valeur de la paire 45.117E est un message en texte libre expliquant la valeur du "code de réponse" de la paire 45.117D.

La paire libellé-valeur 45.117F comporte le libellé "sévérité du logiciel" et la valeur "fatal" ou "avertissement". La valeur de la paire 45.117F indique si le logiciel d'application 210 du client nécessite une mise à jour, mais reste utilisable ("avertissement") ou n'est plus utilisable ("fatal"). La valeur de la paire 45.117F est nulle si le logiciel d'application 210 du client est courant.

La paire libellé-valeur 45.117G comporte le libellé "message de logiciel". La valeur de la paire 45.117G indique des instructions sur ce que doit faire l'utilisateur client 203 dans le cas d'une sévérité du logiciel "fatal" ou "avertissement". La valeur de la paire 45.117G n'est présente que si la valeur de la paire 45.117D n'est pas nulle.

La paire libellé-valeur 45.117H comporte le libellé "honoraire". La valeur de la paire 45.117H indique un honoraire chargé à l'utilisateur client 203, s'il y en a un, qui est associé au message LU1 de traitement de l'ordinateur 100 du serveur. L'honoraire, en cas d'existence, sera déduit du champ 120G.2 du conteneur d'espèces.

La paire libellé-valeur 45.117I comporte le libellé "balance". La valeur de la paire 45.117I indique la balance disponible dans le champ 120G.2 du conteneur d'espèces pour l'utilisateur client 203. Cette balance reflète la balance précédente du conteneur d'espèces ajustée par la valeur du montant de la paire 45.117C chargée via le message LU1 et la valeur des honoraires de la paire 45.117H.

La paire libellé-valeur 45.117J comporte le libellé "session-fonds". La valeur de la paire 45.117J indique le montant transféré par le champ 120G.2 du conteneur d'espèces au champ 130E du montant à l'ouverture de la structure 130 des données de la session du serveur pour toutes les sessions ouvertes.

La paire libellé-valeur 45.117K comporte le libellé "en suspens". La valeur de la paire 45.117K est obtenue à partir du champ 120G.3 de conteneur d'espèces et indique le montant des fonds en attente de transfert à partir de l'instrument lié qui est identifié par la paire 4517E du message LU1 au champ 120G.2 du conteneur d'espèces pour l'utilisateur client 203. Cette valeur représente les fonds qui sont en attente d'agrément ou de traitement par l'émetteur de l'instrument à partir duquel les fonds sont chargés ou chez lequel les fonds sont déchargés.

A l'étape 1412 de la figure 18, le logiciel 110 du serveur assemble le message de réponse LU2 selon l'organigramme de la figure 12. L'opération 1000 d'assemblage de message de serveur a été décrit précédemment pour l'assemblage du message d'annonce R2.

De nouveau en liaison avec la figure 14, le message LU2 est envoyé par l'ordinateur 100 du serveur à l'ordinateur 200 du client à l'étape 1412A.

A l'étape 1413, l'ordinateur 200 du client reçoit le message LU2 en provenance de l'ordinateur 100 du serveur et dévoile le message LU2 en exécutant l'opération 1100 de dévoilement de message (étapes 1101-1121). L'opération 1100 a été décrite précédemment en liaison avec la figure 14 pour le message R2.

A l'étape 1414,

(1) Si un indicateur d'erreur a été établi à l'étape 1105, il sera détecté à l'étape 1414 et le traitement du message LU2 se terminera à l'étape 1415. Au point de vue de l'utilisateur client 203, aucune autre action n'est prise en ce qui concerne le message LU2. Dans la présente invention, un mécanisme est prévu dans le logiciel d'application 210 du client pour créer et envoyer un message à l'ordinateur 100 du serveur. Ce message comprend le message LU2 tel qu'il est reçu par l'ordinateur 200 du client et tout diagnostic sur ce qui a provoqué l'échec du message. Aucune réponse à ce message n'est envoyée par l'ordinateur 100 du serveur à l'ordinateur 200 du client. Au contraire, l'information est utilisée pour estimer s'il y a un problème dans le système et si des mesures de correction appropriées doivent être prises.

(2) Si aucun indicateur d'erreur n'a été établi à l'étape 1105 mais qu'une erreur dans le message LU1 a été détectée à l'étape 905, le traitement se poursuivra à l'étape 1416 dans laquelle le contenu de la paire libellé-valeur 45.117C est vérifié. Si la valeur de la paire 45.117D est autre que "succès", les sous-programmes de traitement d'erreur sont exécutés à l'étape 1418, provoquant l'affichage par le logiciel d'application 210 du client du message contenu dans la paire 45.117E qui est associée au contenu de la paire 45.117D et l'interprétation de la valeur de la paire

44.117D et la prise de toute action qui peut être associée à cette valeur; ou

(3) si le message LU1 a passé la vérification à l'étape 905 et qu'aucun indicateur n'a été établi à l'étape 1105, le traitement se poursuit à l'étape 1419 dans laquelle le logiciel 210 met à jour la base de donnée 202 du client en stockant le contenu du champ de conteneur d'espèces 220J de la structure 220 des données d'état civil du client.

De plus, un nouvel enregistrement 264 de la structure 260 des données du journal du client est créé de la façon suivante : le numéro d'identification d'état civil de la paire libellé-valeur 45.113A est stocké dans le champ 264H. Le numéro de transaction de la paire 45.113B est stocké dans le champ 264B. La date de la paire 45.117B est stocké dans le champ 264C. Le montant de la paire 45.117C est stocké dans le champ 264J. Le code-réponse de la paire 45.117D est stocké dans le champ 264F. Le message de réponse associé au code de réponse du champ 45.117E est stocké dans le champ 264G. Le code de sévérité du logiciel de la paire 45.117F est stocké dans le champ 264D. Le message de logiciel de la paire 45.117G est stocké dans le champ 264E. L'honoraire de la paire 45.117H est stocké dans le champ 264K. La balance de la paire 45.117I est stockée dans le champ 264L.

Le traitement se poursuit à l'étape 1420 dans laquelle l'opération de chargement/déchargement 405 se termine.

E. Opération 407 d'ouverture de session.

La figure 21 décrit un organigramme illustrant l'opération 407 d'ouverture de session qui commence à l'étape 1501.

A l'étape 1502, le logiciel d'application 210 du client indique à l'utilisateur client 203 d'entrer une information relative à la session devant

être créée. Cette information sera incluse dans le message OS1 envoyé à l'ordinateur 100 du serveur et fera partie de la structure 130 des données de session (figure 4H). Dans le mode de réalisation préféré, l'utilisateur client 203 entre la longueur maximum de la durée de la session, le nombre maximum des transactions qui peuvent se produire pendant la session et le montant et la devise des espèces électroniques mises à la disposition de l'utilisateur client 203 pendant la session. L'utilisateur 203 peut aussi entrer une description facultative de la session.

Le message OS1 sera assemblé par et transmis de l'ordinateur 200 du client à l'ordinateur 100 du serveur pour effectuer l'opération 407 d'ouverture de session. Le contenu du message OS1 est maintenant décrit en liaison avec les figures 22A et 22B.

La paire libellé-valeur 4613A comporte le libellé "numéro d'identification". La valeur de la paire 4613A indique le numéro d'identification de l'état civil de l'utilisateur client 203. La valeur de la paire 4613A est obtenue à partir du champ 220A (figure 5C).

La paire libellé-valeur 4613B comporte le libellé "transaction". La valeur de la paire 4613B est un numéro de transaction, produit par le logiciel d'application 210 du client, qui identifie de manière unique le message OS1. La valeur de la paire 4613B permet à l'ordinateur 100 du serveur, lors de la réception du message OS1, (1) d'envoyer un message de réponse associé OS2, qu'on décrit ci-dessous, et (2) de déterminer si le message OS1 est un message dupliqué (c'est-à-dire déjà reçu par l'ordinateur 100 du serveur). La valeur associée à la paire 4613B est stockée dans le champ 256B (figure 5L).

La paire libellé-valeur 4613C comporte le libellé "date". La valeur de la paire 4613B indique la date et l'heure de l'assemblage du message OS1 et est envoyée à l'ordinateur 100 du serveur, conformément à l'horloge de l'ordinateur 200 du client. La valeur

associée à la paire 4613C est stockée dans le champ 256C.

La paire libellé-valeur 4613D comporte le libellé" code de serveur". Comme on le décrit ci-dessous, la paire code DES/VI utilisée par l'ordinateur 200 du client pour crypter la paire opaque 4617 du message OSl est cryptée en utilisant le code public RSA de l'ordinateur 100 du serveur. La valeur de la paire libellé-valeur 4613D est dirigée vers le code privé RSA correspondant qui est stocké dans la structure 160 des données de code privé du serveur.

La paire libellé-valeur 4613E comporte le libellé "catégorie de service". La valeur de la paire 4613E est un libellé qui peut être utilisé pour acheminer le message OSl vers un processeur se trouvant dans l'ordinateur 100 du serveur qui traite les messages d'une catégorie de service particulière.

La paire libellé-valeur 4617 comporte le libellé "opaque". La valeur de la paire 4617 inclut les contenus de la section opaque (sous forme cryptée) du message OSl. On décrira maintenant les contenus de la section opaque du message OSl, représentés en figure 22B.

La paire libellé-valeur 4617A comporte le libellé "type". La valeur de la paire 4617A se rapporte à un enregistrement dans la structure 150 des données de message qui établit les libellés des contenus de la section opaque du message OSl. La valeur de la paire 4617A est obtenue à partir du logiciel d'application 210 du client qui produit le libellé lorsque l'utilisateur client 203 amorce l'opération 407 d'ouverture de session.

La paire libellé-valeur 4617B comporte le libellé "date de serveur". La valeur de la paire 4617B indique la date et l'heure de l'assemblage du message OSl telles qu'elles sont mesurées par la perception par l'ordinateur 200 du client de l'horloge de l'ordinateur 100 du serveur.

La paire libellé-valeur 4617C comporte le libellé "version de logiciel". La valeur de la paire 4617C indique la version du logiciel d'application 210 du client qui communique avec l'ordinateur 100 du serveur. La valeur de la paire 4617C est obtenue à partir de la donnée incorporée dans le logiciel d'application 210. La valeur associée à la paire 4617C est stockée dans le champ 256D.

La paire libellé-valeur 4617D comporte le libellé "enregistrement-note". La valeur de la paire 4617D est une note facultative en texte court devant être stockée dans le champ 130M (figure 4H). Par exemple, la note peut indiquer "Achat de Noël" ou "équipement de ski". La valeur de la paire 4617D est obtenue à partir de la réponse de l'utilisateur client 203 à une demande du logiciel d'application 210 du client et est de préférence limitée à soixante caractères afin de simplifier l'affichage produit par le logiciel 210.

La paire libellé-valeur 4717E comporte le libellé "montant" et la valeur entrée à l'étape 1502 indiquant le montant maximum des espèces électroniques disponibles pour l'utilisateur client 203 pendant la session. La valeur associée à la paire 4517E est stockée dans le champ 256F.

La paire libellé-valeur 4617F comporte le libellé "durée de vie de code" et la valeur entrée à l'étape 502 indiquant la durée maximum de la session est telle qu'elle est demandée par le client utilisateur 203. La valeur associée à la paire 4617F est stockée dans le champ 256H.

La paire libellé-valeur 4617G comporte le libellé "limite d'utilisation de code" et la valeur entrée à l'étape 1502 indiquant le nombre maximum des transactions qui peuvent se produire pendant la session telles qu'elles sont demandées par l'utilisateur client 203. La valeur associée à la paire 4617G est stockée dans le champ 256G.

La paire libellé-valeur 4617H comporte le libellé "code". La valeur de la paire 4617H représente un contrôle de total de somme du modulus de la paire code public RSA/code privé de l'état civil 120.1 du client. La valeur de la paire 4617H permet à l'ordinateur 100 du serveur de confirmer que le code public RSA maintenu dans le champ 120B (figure 4B) est le même que celui utilisé pour signer le message OS1 (paire libellé-valeur 4617I).

La paire libellé-valeur 4617I comporte le libellé "signature". La valeur de la paire 4617I représente la signature numérique pour l'état civil 120.1 du client. Pour le message OS1, la valeur de la paire 4617I est un contrôle de total de somme des paires 4613A-4613D et des paires 4617A-4617H dans l'ordre alphabétique, chiffrées avec le code privé RSA pour l'état civil 120.1. Le code privé RSA pour l'état civil 120.1 est obtenu à partir du champ 220H (figure 5C).

Le message OS1 est assemblé en utilisant l'opération 800 d'assemblage de message (figure 9) qu'on a décrite précédemment pour l'assemblage du message d'inscription R1. La modification suivante est notée pour le message OS1 : une copie de message OS1 est de préférence sauvegardée dans le champ 256I.

Dans le cas de l'assemblage du message OS1 par l'ordinateur 300 du commerçant, un nouvel enregistrement 370.1 (figure 7C) est créé de la façon suivante :

La valeur de la paire 4613B est stockée dans le champ 370P. La valeur de la paire 4617F est stockée dans le champ 370Q. La valeur de la paire est stockée dans le champ 370R. La valeur du champ d'état 3700 est établie à "tentative" par le logiciel d'application 310 du commerçant.

De nouveau en liaison avec la figure 15, l'opération 407 d'ouverture de session se poursuit à l'étape 1504. Là, l'ordinateur 200 du client transmet le message OS1 à l'ordinateur 100 du serveur. L'ordinateur

200 du client attend un message de réponse OS2 de la part de l'ordinateur 100 du serveur.

A l'étape 1505, l'ordinateur 100 du serveur reçoit le message OS1 en provenance de l'ordinateur 200 du client et dévoile le message OS1 en exécutant l'opération 900 de dévoilement de message du serveur. L'opération 900 (étapes 901-917) a été décrite précédemment pour le message R1 en liaison avec la figure 11. On notera la modification suivante : une copie du message OS1 est stockée dans le champ 140E (figure 4L).

A l'étape 1506, si l'un des tests des étapes 909A, 912, 914, 915 ou 916 a provoqué l'établissement d'un indicateur d'erreur à l'étape 905, les opérations de traitement des erreurs sont exécutées par l'ordinateur 100 du serveur à l'étape 1514. Alors que le niveau du traitement des erreurs à l'étape 1514 est largement une décision administrative, on préfère qu'au minimum, les échecs du total de contrôle, de la signature, et de la forme, et un retour "fatal" du mode opératoire de vérification du logiciel se traduisent par un message de retour contenant un code qui peut être traité par le logiciel d'application 210 du client et par un message qui peut être lu par l'utilisateur client 203. L'opération de traitement des erreurs de l'étape 1514 implique l'association d'un indicateur avec un code d'erreur spécifique (qu'on décrit dans le contexte du message de retour OS2 ci-après) et la création d'un message en texte (soit à partir d'une structure de données de messages ou d'un message envoyés par l'administrateur du système). L'ordinateur 100 du serveur produit alors un message OS2 similaire à celui décrit ci-dessous pour l'ordinateur 200 du client, acheminant le code d'erreur et tout message concerné.

Si les tests des étapes 909A, 912, 914, 915 et 916 n'ont pas provoqué l'établissement d'un indicateur d'erreur à l'étape 905, le traitement se poursuit à l'étape 1507. Là, l'ordinateur 100 du serveur

calcule un numéro d'identification de session, un code de chiffrement/déchiffrement de session ("code de session") et un sel de session et valide les limites de la session demandées par l'utilisateur client 203 comme cela est reflété dans le message OS1.

Le numéro d'identification de session est une quantité de 64 bits qui identifie de manière unique la session qui est créée. L'aspect unique est assuré car les numéros d'identification de session sont produits séquentiellement par l'ordinateur 100 du serveur.

Le code de session est une quantité de 128 bits contenant un code DES de 56 bits (64 bits avec le bit de poids faible de chaque octet ignoré) et un vecteur d'initialisation de 64 bits.

Le sel de session est un sel cryptographique de 8 octets utilisé pour renforcer l'authentification des messages CA1-CA4 qui sont échangés lors d'une session. On décrira ultérieurement les messages CA1-CA4.

Les limites de la session demandées par le client utilisateur 203 sont la valeur de la quantité de la paire libellé-valeur 4617E, la valeur de la durée de vie du code de la paire 4617F, et la valeur de la limite d'utilisation du code de la paire 4617G. S'agissant de la durée de vie du code et de la limite d'utilisation du code, on préfère que ces valeurs soient soumises à une gamme fixe établie par l'ordinateur 100 du serveur de manière à améliorer l'efficacité du système et à rendre maximale la sécurité des transactions exécutées lors d'une session. L'ordinateur 100 du serveur vérifie que les valeurs demandées se trouvent dans de telles limites. Toute limite demandée qui dépasse une valeur permise est ignorée et la valeur maximum permise est la valeur imposée par l'ordinateur 100.

La valeur de la paire libellé-valeur 4617E représente le montant des fonds électroniques que l'utilisateur client 203 désire dépenser pendant la session. Le montant réel de ces fonds mis à la disposition de l'utilisateur 203 lors d'une session peut

être inférieur ou égal au montant demandé par l'utilisateur 203 à l'étape 1502. Par exemple, l'utilisateur client peut demander plus d'espèces électroniques que celles qui sont disponibles dans le champ 120G.2 du conteneur d'espèces pour l'utilisateur client 203. Dans ce cas, le montant accordé, tel qu'indiqué par la paire libellé-valeur 4717I décrite ci-dessous, est limité au montant stocké dans le champ 120G.2 pour l'utilisateur 203.

A l'étape 1508, la structure 130 des données de session du serveur (figure 4H) est mise à jour. Le numéro d'identification de session est stocké dans le champ 130A de numéro d'identification de session. Le code de session est stocké dans le champ 130B. Le sel de session est stocké dans le champ 130C. Le montant des espèces électroniques mis à la disposition de l'utilisateur client 203 pendant la session est stocké dans le champ d'ouverture de montant 130E et le désignateur de devise associé à la valeur stockée dans le champ 130E est stocké dans le champ 130D. Initialement, le champ 130F reflète la valeur du montant à l'ouverture dans le champ 130E. Alors qu'il y a consommation des espèces électroniques, la valeur du champ 130F reflète la différence entre le montant à l'ouverture et le montant consommé. La durée de vie du code accordée réellement par l'ordinateur 100 du serveur est stockée dans le champ 130J. La limite d'utilisation de code réellement accordée par l'ordinateur 100 est stockée dans le champ 130I. La valeur de la paire 4613A est stockée dans le champ 130K. La date de la création de la session est obtenue à partir du logiciel d'application 110 du serveur et est stockée dans le champ de date d'ouverture 130G. La valeur de la paire libellé-valeur 4617D est sauvegardée dans le champ 130M de note d'enregistrement. Les autres champs de la structure 130 des données d'une session de serveur sont discutés dans le contexte des messages du type CA donnés ci-après.

Après l'étape 1509, le message OS2 est assemblé par et transmis de l'ordinateur 100 du serveur à l'ordinateur 200 du client pour achever l'opération 407 de la session de crédit. Les contenus du message OS2 seront maintenant décrits en liaison avec les figures 23A et 23B.

La paire libellé-valeur 4713A comporte le libellé "numéro d'identification". La valeur de la paire 4713A indique le numéro d'identification d'état civil pour le client utilisateur 203. La valeur de la paire 4713A est la même que celle reçue dans le message OS1 dans la paire 4613A.

La paire libellé-valeur 4713B comporte le libellé "transaction". La valeur de la paire 4713B est un numéro de transaction. La valeur de la paire 4713B est la même que celle reçue dans le message OS1 dans la paire 4613B.

La paire libellé-valeur 4713C comporte le libellé "date". La valeur de la paire 4713C est la même que celle qui a été reçue dans le message OS1 dans la paire 4613C.

La paire libellé-valeur 4713D comporte le libellé "catégorie de service". La valeur de la paire 4713D est la même que celle reçue dans la paire 4613E du message OS1.

La paire libellé-valeur 4717 comporte le libellé "opaque". La valeur de la paire 4717 comporte les contenus de la section opaque (sous forme chiffrée) du message OS2. On décrira maintenant les contenus de la section opaque du message OS2 représentés en figure 23B.

La paire libellé-valeur 4717A comporte le libellé "type". La valeur de la paire 4717A se rapporte à un enregistrement dans la structure 270 des données de message (figure 5A) qui établit les libellés du contenu de la section opaque du message OS2. La valeur de la paire 4717A est obtenue à partir du logiciel 110 du serveur.

La paire libellé-valeur 4717B comporte le libellé "date de serveur". La valeur de la paire 4717B indique la date et l'heure de l'assemblage du message OS2 en conformité avec l'horloge de l'ordinateur 100 du serveur.

La paire libellé-valeur 4717C comporte le libellé "code de réponse" et la valeur "succès" ou "échec" comme on l'a décrit précédemment. La valeur de la paire 4717C indique si l'opération 407 d'ouverture de session a été un succès ou un échec.

La paire libellé-valeur 4717D comporte le libellé "sévérité du logiciel" et la valeur "fatal" ou "avertissement". La valeur de la paire 4717D indique si le logiciel d'application 210 du client doit être mis à jour, mais reste valable ("avertissement") ou n'est plus utilisable ("fatal"). La valeur de la paire 4717D est nulle si le logiciel 210 est courant.

La paire libellé-valeur 4717E comporte le libellé "message de logiciel". La valeur de la paire 4717E indique des instructions sur ce que doit faire l'utilisateur client 203 en cas de sévérité "fatal" ou "avertissement" du logiciel. La valeur de la paire 4717E n'est présente que si la valeur de la paire 4717D n'est pas nulle.

La paire libellé-valeur 4717F comporte le libellé "message". La valeur de la paire 4517F est un message en texte libre qui est associé à une condition d'erreur ou de succès et renvoyée dans la paire 4717C et affichée pour l'utilisateur client 203. La valeur de la paire 4317F peut incorporer un message indiquant un numéro d'identification d'état civil demandé se trouvant en double, une mauvaise signature numérique ou un message OS1 mal formé et des instructions sur ce que doit faire l'utilisateur client 203 (par exemple "appeler l'administrateur du système").

La paire libellé-valeur 4717G comporte le libellé "durée de vie du code" et la valeur obtenue à

partir de la durée de vie du code du champ 130K (figure 4L) indiquant le temps maximum que durera la session.

La paire libellé-valeur 4717H comporte le libellé "limite d'utilisation de code" et la valeur obtenue à partir de la limite d'utilisation de code du champ 130J indiquant le nombre maximum des transactions qui peuvent se produire pendant la session.

La paire libellé-valeur 4717I comporte le libellé "montant" et indique le montant maximum des espèces électroniques mises à la disposition de l'utilisateur client 203 pendant la session. La valeur du montant de la paire 4717I peut être inférieure ou égale au montant demandé par l'utilisateur client 203 à l'étape 1502.

La paire libellé-valeur 4717J comporte le libellé "change étranger" et une valeur indiquant un taux de conversion à partir de la dénomination de la devise qui est incluse dans la valeur de la paire 4217I en d'autres devises, par exemple, des dollars américains en dollars canadiens. De préférence, le taux de conversion indiqué est le nombre des unités mineures (ou des unités majeures s'il n'y a pas d'unité mineure) de la devise de destination pour cent unités majeures de la devise source.

La paire libellé-valeur 4717K comporte le libellé "fonds de session". La valeur de la paire 4717K indique un montant des espèces électroniques envoyé à toutes les sessions ouvertes dont la valeur du montant de la paire 4417I. Un état civil de client 120.1 peut avoir n'importe quel nombre de sessions qui sont ouvertes. La paire 4717K fournit à l'utilisateur client 203 une information relative au montant des fonds alloué initialement à toutes les sessions ouvertes, dont la session venant d'être ouverte.

La paire libellé-valeur 4717L comporte le libellé "balance". La valeur de la paire 4717L indique le montant des espèces électroniques stocké dans le champ 120G.2 du conteneur d'espèces de la structure 120

des données d'état civil de serveur pour l'utilisateur client 203 après le transfert de fonds en espèces électroniques au champ du montant à l'ouverture 130E de la structure 130 des données de session du serveur.

La paire libellé-valeur 4717M comporte le libellé "en suspens". La valeur de la paire 4717M est obtenue à partir du champ 120G.3 de conteneur d'espèces et indique le montant des espèces électroniques non-recueillies qui sont encore dégagées dans l'état civil 120.1 pour l'utilisateur client 203. Cette valeur représente des espèces électroniques qui sont en attente d'accord ou de traitement par l'émetteur de l'instrument financier, à partir duquel des fonds sont chargés ou vers lequel des fonds sont déchargés.

La paire libellé-valeur 4717N comporte le libellé "honoraire". La valeur de la paire 4717N indique un honoraire facturé à l'utilisateur client 203, s'il y en a un, qui est associé au message de traitement OS1.

La paire libellé-valeur 47170 comporte le libellé "numéro d'identification de session". La valeur de la paire 47170 est obtenue à partir du numéro d'identification de session du champ 130A.

La paire libellé-valeur 4717P comporte le libellé "code de session". La valeur de la paire 4717P est obtenue à partir du code de session du champ 130B.

La paire libellé-valeur 4717Q comporte le libellé "sel de session". La valeur de la paire 4717Q est obtenue à partir du sel de session du champ 130C.

A l'étape 1509 de la figure 21, le logiciel 100 du serveur assemble le message OS2 en conformité avec l'organigramme de la figure 12. L'opération 1000 de l'assemblage des messages du serveur a été décrite précédemment pour l'assemblage du message R2.

A l'étape 1509A, le message OS2 est envoyé de l'ordinateur 100 du serveur à l'ordinateur 200 du client.

A l'étape 1510, l'ordinateur 200 du client reçoit un message OS2 en provenance de l'ordinateur 100

du serveur et dévoile le message OS2 en exécutant l'opération 1100 de dévoilement de message en ce qui concerne le message OS2. L'opération 1100 (étapes 1101-1121) a été décrite précédemment pour le message R2 en liaison avec la figure 14.

A l'étape 1511,

(1) Si un indicateur d'erreur a été établi à l'étape 1505, il sera détecté à l'étape 1511 et le traitement du message OS2 se termine à l'étape 1512. Au point de vue de l'utilisateur client 203, aucune autre action n'est prise en ce qui concerne le message OS2. Dans la présente invention, un mécanisme est prévu dans le logiciel d'application 210 du client pour créer et envoyer un message à l'ordinateur 100 du serveur. Ce message incorpore le message OS2 tel qu'il est reçu par l'ordinateur 200 du client et tout diagnostic de ce qui a pu provoquer l'échec du message. Aucune réponse à ce message n'est envoyée par l'ordinateur 100 du serveur à l'ordinateur 200 du client. Au contraire, l'information est utilisée pour indiquer s'il existe un problème dans le système et si des mesures de corrections appropriées doivent être prises.

(2) Si aucun indicateur d'erreur n'a été établi à l'étape 1105 mais qu'une erreur dans le message OS1 a été détectée à l'étape 905, le traitement se poursuivra à l'étape 1513 dans laquelle le contenu de la paire libellé-valeur 4717C est vérifié. Si la valeur de la paire 4717C est autre que "succès", les sous-programmes de traitement d'erreur sont exécutés à l'étape 1515, et font que le logiciel d'application 210 du client affiche le message contenu dans la paire 4717F associée au contenu de la paire 4517C et interprète la valeur de la paire 4717C et prend toute action qui peut être associée à cette valeur; ou

(3) si le message OS1 a passé la vérification à l'étape 905 et qu'aucun indicateur n'a été établi à l'étape 1105, le traitement se poursuit à

l'étape 1516 dans laquelle le logiciel d'application 210 du client met à jour la base de donnée 202 du client.

La structure 240 des données de session d'un client est mise à jour de la façon suivante :

le numéro d'identification de session est stocké dans le champ 240. Le code de session est stocké dans le champ 240B. Le sel de session est stocké dans le champ 240C. La valeur de la paire 4717I comprend un désignateur de devise et une quantité. La valeur de la quantité est stockée dans le champ de quantité à l'ouverture 130E et le désignateur de devise associé à la valeur stockée dans le champ 130E est stockée dans le champ 130D. La valeur de la paire 4717G est stockée dans le champ de durée de vie de code 240K. La valeur de la paire 4717G est stocké dans le champ limite d'utilisation de code 240J.

On remarquera que le champ 240F reflètera initialement la valeur du montant à l'ouverture du champ 240E. Alors que des espèces électroniques sont consommées, la valeur dans le champ 240F reflètera la différence entre le montant à l'ouverture et le montant consommé. Les autres champs de la structure 240 des données d'une session de client sont discutés dans le contexte des messages du type CA dans ce qui suit.

En plus des valeurs enregistrées dans la structure 240 des données d'une session de client, l'enregistrement 265 de la structure 260 des données du journal du client est mis à jour de la façon suivante : le numéro d'identification d'état civil de la paire libellé-valeur 4713A est stocké dans le champ 265H. Le numéro de transaction de la paire 4713B est stocké dans le champ 265B. La date de la paire 4717B est stockée dans le champ 265C. Le code de réponse de la paire 4717C est stocké dans le champ 265F. Le code de sévérité du logiciel de la paire 4717D est stocké dans le champ 265D. Le message de logiciel de la paire 4717E est stocké dans le champ 265E. Le message de réponse associé au code de réponse du champ 4717F est stocké dans le

champ 265G. La durée de vie de code de la paire 4717G est stockée dans le champ 265K. La limite d'utilisation de code de la paire 4717H est stockée dans le champ 265J. Le montant de la paire 4717I est stocké dans le champ 265I. La balance de la paire 4717L est stockée dans le champ 265P. L'honoraire de la paire 4717N est stocké dans le champ 2650. Le numéro d'identification de session de la paire 47170 est stocké dans le champ 265L.

Si l'opération d'ouverture de session est amorcée par l'utilisateur commerçant 303, l'enregistrement 370.1 de la structure 370 des données du journal des espèces du commerçant est mis à jour de la façon suivante :

Le code de réponse de la paire 4717C est stocké dans le champ 3700. Le message de la paire 4717F associé au code de réponse de la paire 4717C est sauvegardé dans le champ 370T. Le numéro d'identification de session de la paire 47170 est stocké dans le champ 370S.

Le traitement se poursuit à l'étape 1517 dans laquelle se termine l'opération 407 d'ouverture de session.

F. Opération 409 de transaction/paiement.

Lorsque l'utilisateur client 203 et l'utilisateur commerçant 303 ont ouvert des sessions, des transactions sûres quant aux espèces peuvent se produire par l'Internet 50. La sécurité signifie dans ce contexte que l'utilisateur client 203 et l'utilisateur commerçant 303 peuvent avoir confiance que leurs fonds électroniques ne risquent pas d'être accédés par un tiers non autorisé et qu'aucune espèce électronique ne sera transférée à moins que les deux parties n'aient été d'accord sur une transaction qui a été validée par l'ordinateur 100 du serveur.

Une transaction comprend un utilisateur client 203 faisant des achats parmi les utilisateurs

commerçants 303 de l'Internet qui ont des états civils 120.2 de commerçant. En utilisant des techniques bien connues l'utilisateur client 203 et un utilisateur commerçant 303 se mettent d'accord sur le prix que l'utilisateur 203 est prêt à payer pour un produit devant être fourni par l'utilisateur 303. Lorsque l'utilisateur commerçant 303 demande le paiement, l'utilisateur client 203 choisit de payer avec des espèces électroniques. Ce choix provoque un échange de messages qui se traduit par le paiement final à l'utilisateur commerçant 303 du produit acheté par l'utilisateur client 203.

Les figures 24A-24C représentent un organigramme décrivant l'opération 409 de transaction/paiement qui commence à l'étape 1701.

A l'étape 1702A, l'ordinateur 300 du commerçant assemble le message PR1. Le message PR1 ne comporte pas de préférence des données cryptées. Ainsi, seules les étapes 814-817 de l'opération 800 d'assemblage de message (figure 9) sont nécessaires pour assembler le message PR1. Le contenu du message PR1 sera maintenant décrit en liaison avec la figure 25.

La paire libellé-valeur 5013A comporte le libellé "type". La valeur de la paire 5013A se rapporte à un enregistrement dans la structure 270 des données de message (figure 5A) qui établit des libellés comprenant PR1. La valeur de la paire 5013A est obtenue à partir du logiciel d'application 310 du commerçant.

La paire libellé-valeur 5013B comporte le libellé "numéro d'identification de commerçant". La valeur de la paire 5013B indique le numéro d'identification d'état civil pour l'utilisateur commerçant 303. La valeur de la paire 5013B est obtenue à partir du champ 320A (figure 6C).

La paire libellé-valeur 5013C comporte le libellé "numéro d'identification d'ordre de commerçant". La valeur de la paire 5013C indique un numéro d'identification d'ordre produit par l'ordinateur 300 du

commerçant pour identifier un ordre particulier. La valeur de la paire 5013C est stockée dans le champ 370C (figure 7C).

La paire libellé-valeur 5013D comporte le libellé "date de commerçant". La valeur de la paire 5013D indique la date et l'heure de l'assemblage du message PR1 conformément à l'horloge de l'ordinateur 300 du commerçant.

La paire libellé-valeur 5013E comporte le libellé "version du logiciel du commerçant". La valeur de la paire 5013E indique la version du logiciel d'application 310 du commerçant qui communique avec l'ordinateur 200 du client. La valeur de la paire 5013E est obtenue auprès du logiciel d'application 310 du commerçant.

La paire libellé-valeur 5013F comporte le libellé "note". La valeur de la paire 5013F décrit le produit qui est fourni par l'utilisateur commerçant 303 à l'utilisateur client 203. La valeur de la paire 5013F est obtenue par le logiciel d'application 310 du commerçant à partir du logiciel fourni par le commerçant 303 ou par un tiers.

La paire libellé-valeur 5013G comporte le libellé "montant du commerçant". La valeur de la paire 5013G décrit la devise et le prix pour le produit décrit dans la paire 5013F.

La paire libellé-valeur 5013H comporte le libellé "acceptations". La valeur de la paire 5013H identifie les cartes de crédit acceptées par l'utilisateur commerçant 303 (s'il y en a). Les valeurs de la paire 5013H sont obtenues auprès de l'utilisateur commerçant 303.

La paire libellé-valeur 5013I comporte le libellé "RRU à payer à". La valeur de la paire 5013I est un releveur des ressources uniformes de l'Internet 50. Le releveur de la paire 5013I est l'adresse sur l'Internet 50 à laquelle l'ordinateur 200 du client doit envoyer le message CA1, qu'on décrit ultérieurement.

La paire libellé-valeur 5013J comporte le libellé "annulation de RRU". La valeur de la paire 5013J est un releveur de ressources uniformes de l'Internet 50. Ce releveur de la paire 5013J est utilisé par l'ordinateur 200 du client dans le cas où l'utilisateur client 203 décide d'annuler une transaction.

La paire libellé-valeur 5013K comporte le libellé "RRU-succès". La valeur de la paire 5013K est un relèveur de ressources uniformes de l'Internet 50 qui dirige l'ordinateur 200 du client vers une adresse dans le web mondial si une transaction est réussie. Le succès d'une transaction est rapporté dans le message CA4, qu'on décrit ultérieurement. Par exemple, si la transaction est validée par l'ordinateur 100 du serveur, la valeur de la paire 5013K peut diriger l'ordinateur 200 du client vers une page du web qui félicite l'utilisateur client 203 de son achat.

La paire libellé-valeur 5013L comporte le libellé "RRU-échec". La valeur de la paire 5013L est un releveur de ressources uniformes de l'Internet 50 qui dirige l'ordinateur 200 du client vers une adresse du web mondial si une transaction n'a pas réussi. L'échec d'une transaction est rapporté dans le message CA4, qu'on décrit ultérieurement. Par exemple, si la transaction n'est pas validée par l'ordinateur 100 du serveur, la valeur de la paire 5013L peut diriger l'ordinateur 200 du client vers une page du web qui demande à l'utilisateur client 203 d'essayer de nouveau son achat.

La paire libellé-valeur 5013M comporte le libellé "code de contrôle de total de somme signé par le commerçant". La valeur de la paire 5013M représente un contrôle de total de somme de la partie modulus de la paire code public RSA/code privé utilisée par l'ordinateur 300 du commerçant pour signer le contrôle de total de somme de la paire 5013N qu'on décrit ci-dessous. La valeur de la paire 5013M permet à l'ordinateur 100 du serveur de confirmer que le code

public RSA maintenu dans le champ 120CC (figure 4E) pour l'état civil 120.2 du commerçant est le même code qui a été utilisé pour signer la paire "contrôle de total de somme signé par le commerçant" 5013N, ou si le décryptage de la paire 5013N est un échec, la raison d'un tel échec.

La paire libellé-valeur 5013N comporte le libellé "contrôle de total de somme signé par le commerçant". Pour le message PR1, la valeur de la paire 5013N est un contrôle de total de somme des paires 5013A-5013M dans cet ordre. Ce contrôle de total de somme est signé, signifiant que ce contrôle est de nouveau effectué, puis crypté avec le code privé RSA pour l'état civil 120.2 du commerçant. L'état civil 120.2 est obtenu à partir du champ 320H (figure 6C).

La paire libellé-valeur 50130 comporte le libellé " commerçant-montant 2". La valeur de la paire 50130 décrit le prix en devises autres que celle associée au prix spécifié dans la paire 5013G.

L'utilisateur client 203 ne peut authentifier la signature de la paire 5013N car il n'a pas le code public pour l'état civil 120.2 du commerçant. La valeur de la paire 5013N peut être stockée par le logiciel d'application du client dans le cas où il se produit un différend sur la transaction. Dans ce cas, l'ordinateur 100 du serveur peut utiliser la valeur de la paire 5013N pour déterminer si le message PR1 a été réellement envoyé par l'ordinateur 300 du commerçant.

De nouveau en liaison avec la figure 24A, étape 1705A, un nouvel enregistrement 350.1 (figure 7) est ajouté comme suit :

La valeur de la paire 5013C (relative au numéro d'identification d'ordre du commerçant) est stockée dans le champ numéro d'identification d'ordre 350A.

La valeur de la paire libellé-valeur 5013G (relative au montant que l'utilisateur commerçant 303 a

l'intention de recevoir en échange pour des produits) est stockée dans le champ de montant 350B.

L'opération 409 de transaction/paiement se poursuit à l'étape 1702C. Là, l'ordinateur 300 du commerçant transmet le message PR1 à l'ordinateur 200 du client. L'ordinateur 300 du commerçant attend le message CA1 en provenance de l'ordinateur 200 du client.

A l'étape 1702D, l'ordinateur 200 du client reçoit le message PR1 en provenance de l'ordinateur 300 du commerçant et dévoile le message PR1 en exécutant l'opération 3300 de dévoilement de message. L'opération 3300 sera maintenant décrite en liaison avec la figure 26, où elle commence à l'étape 3301.

A l'étape 3302, le logiciel d'application 210 du client extrait le numéro de protocole de l'en-tête 5005 du message PR1. Ensuite, sur la base du numéro de protocole extrait, la structure 270 des données de grille de message (figure 5A) est accédée pour déterminer le format attendu du message PR1. Le format attendu peut comprendre une syntaxe de message (par exemple caractères de fin de ligne permis) et codage de message (par exemple ASCII ou hex). Le message PR1 est analysé en conformité avec le format attendu de la façon suivante.

A l'étape 3303, l'ordinateur 200 du client calcule un total de contrôle en utilisant la même donnée que celle utilisée par l'ordinateur 300 du commerçant. A l'étape 3304A, le total de contrôle calculé à l'étape 3303 est comparé au total de contrôle de la queue 5050 du message PR1. Si les totaux ne sont pas égaux, le message PR1 est écarté à l'étape 3304B dans laquelle l'opération de dévoilement 3300 se termine aussi.

Si les totaux de contrôle sont égaux à l'étape 3304A, le traitement se poursuit à l'étape 3304C dans laquelle le message est vérifié pour déterminer s'il est approprié à l'opération 3300 de dévoilement de message. Si un message incorpore le libellé "type" dans la partie transparente du message et la valeur PR1, il

est approprié. Si un message ne comporte pas cette paire libellé-valeur, il n'est pas approprié pour l'opération 3300 auquel cas le traitement se poursuit à l'étape 3304D dans laquelle le message est dévié vers une autre opération de dévoilement, qu'on décrit ultérieurement. Le message PR1 est approprié; par conséquent, le traitement se poursuit à l'étape 3304E dans laquelle le type de message est déterminé par référence à la valeur de la paire libellé-valeur 5013A. Dans ce cas, la valeur de la paire est "demande de paiement".

A l'étape 3305, une vérification de forme du message PR1 est exécutée. L'opération de vérification de forme de l'étape 3305 dépend de la version du logiciel. Plus précisément, le format attendu du message, et les critères qui déterminent s'il est acceptable, dépendent du message et de toute variante de message qui est valable à un instant donné. Au minimum, l'opération de vérification de forme établira si un message entrant contient tous les libellés qui sont prescrits pour ce message, si des valeurs pour chaque libellé nécessitent ou non une valeur, et si les valeurs sont ou non du type (par exemple texte, nombres signés), syntaxe et à l'intérieur de toutes limites spécifiées selon nécessité. S'il y a des libellés additionnels, l'ordinateur 200 du client les ignorera. Si un message ne peut être analysé, ou s'il peut être analysé mais ne satisfait pas un critère de forme, un indicateur d'erreur sera établi à l'étape 3306. Dans ce cas, l'opération 3300 de dévoilement de message se termine à l'étape 3309.

Si le message PR1 a la forme correcte, le traitement se poursuit à l'étape 3307. Là, le logiciel d'application 210 du client ajoute un nouvel enregistrement 266 comme suit :

La valeur du numéro d'identification du commerçant de la paire 5013B est stockée dans le champ 266A. La valeur du numéro d'identification d'ordre du commerçant de la paire 5013C est stockée dans le champ

266B. La valeur du montant de la paire 5013G est stockée dans le champ 266C. La valeur "commerçant-note" de la paire 5013F est stockée dans le champ 266. Le "payer à RRU" est stocké dans le champ 266F.

L'opération 3300 de dévoilement de message se termine à l'étape 3309.

De nouveau en liaison avec la figure 24, à l'étape 1703, l'ordinateur 200 du client affiche l'offre de l'utilisateur commerçant 303 pour l'utilisateur client 203. Les valeurs de la paire 5213F et de la paire 5213G (décrivant le produit vendu à l'utilisateur client 203 et le prix de l'offre) sont affichées.

A l'étape 1704, l'utilisateur client 203 accepte l'offre de l'utilisateur commerçant 303. Il est prévisible qu'à ce moment critique, l'utilisateur client 203 recevra aussi diverses options de paiement (par exemple carte de crédit ou espèces électroniques). Si l'utilisateur client 203 choisit la carte de crédit, d'autres opérations auront lieu qu'on ne décrit pas ici). Si l'utilisateur 203 indique son désir de payer le produit avec des espèces électroniques, le traitement se poursuit à l'étape 1705.

A l'étape 1705, le logiciel d'application 210 du client détermine si l'utilisateur client 203 a une session ouverte en recherchant les enregistrements 240 (figure 5).

Si l'utilisateur client 203 n'a pas une session ouverte, le traitement se poursuit à l'étape 1706. Là, une session est créée en utilisant l'opération 405 d'ouverture de session qu'on a décrite ci-dessus.

Si l'utilisateur client 203 a une session ouverte, ou après l'exécution d'une opération 405 d'ouverture de session, le traitement se poursuit à l'étape 1707A. Là, l'ordinateur 200 du client assemble le message CA1 de la façon suivante.

En liaison avec la figure 27, le mode opératoire CA12 d'assemblage de message est décrit. ("CA12" concerne le fait que ce mode opératoire

d'assemblage de message est exécuté pour assembler les messages CA1 et CA2).

L'opération CA12 d'assemblage de message pour le message CA1 commence à l'étape 1621. Le message CA1 est représenté en figures 28A et 28B.

A l'étape 1622, le logiciel d'application 210 du client accède à la structure 270 des données de grille de message (figure 5A) afin d'obtenir une liste de libellés, qui, lorsqu'ils correspondent à des valeurs associées, constituent les paires libellé-valeur transparentes 5113A-5113I du message CA1. A l'étape 1623, des valeurs sont associées à chaque libellé. On décrira maintenant ces paires libellé-valeur.

La paire libellé-valeur 5113A comporte le libellé "type". La valeur de la paire 5113A concerne un enregistrement dans la structure 150 des données de message (figure 4A) qui établit des libellés comprenant le message CA1. La valeur de la paire 5113A est obtenue à partir du logiciel d'application 210 du client.

La paire libellé-valeur 5113B comporte le libellé "version". La valeur de la paire 5113B est un code maintenu dans la structure 270 des données de message (figure 5A) qui se rapporte à un enregistrement parmi les enregistrements de type indiqués par la paire 5113A. La valeur de la paire 5113B est récupérée par le logiciel d'application 210 du client auprès de la structure 270 des données de message.

La paire libellé-valeur 5113C comporte le libellé "numéro d'identification de session". La valeur de la paire 5113C est obtenue à partir du numéro d'identification de session du champ 240A (figure 5E).

La paire libellé-valeur 5113D comporte le libellé "indice". La valeur de la paire 5113D est un nombre entier affecté par le logiciel d'application 210 du client à une transaction se produisant pendant une session et représente une utilisation du code de session stocké dans le champ 240B. La gamme des valeurs est

limitée par 1 et la limite d'utilisation de code stockée dans le champ 240J.

La paire libellé-valeur 5113E comporte le libellé "devise du payeur" et la valeur indiqué par la partie devise de la paire 5113G du message PR1. La valeur de la paire 5113E décrit la devise dans laquelle l'utilisateur commerçant 303 a l'intention d'être payé pour la transaction.

La paire libellé-valeur 5113F comporte le libellé "note-contrôle de total de somme". La valeur de la paire 5113F est un contrôle du total de somme de la paire 5013F du message PR1.

La paire libellé-valeur 5113G comporte le libellé "payeur-numéro d'identification". La valeur de la paire 5113G est le numéro d'identification d'état civil du commerçant obtenu d'après la valeur de la paire 5113B du message PR1.

La paire libellé-valeur 5113H comporte le libellé "ordre-numéro d'identification". La valeur de la paire 5113H est le numéro d'identification d'ordre obtenu d'après la valeur de la paire 5113C du message PR1.

La paire libellé-valeur 5113I comporte le libellé "catégorie de service". La valeur de la paire 5113I est un libellé qui peut être utilisé par l'ordinateur 300 du commerçant pour acheminer le message CA1 vers un processeur de l'ordinateur 300 du commerçant qui traite les messages d'une catégorie de service particulière.

A l'étape 1624, le logiciel d'application 210 du client produit un DES-CA1 du code DES de 56 bits conformément à l'opération 1600 de production de code CA-DES, représentée dans l'organigramme de la figure 16D.

La production du DES-CA1 du code DES commence à l'étape 1610.

A l'étape 1610, le logiciel d'application 210 du client construit une quantité Q, quantité à

octet. La quantité Q est un chaînage des valeurs des paires 5113A, 5113B et 5113D du message CA1. On préfère que le code DES obtenu change avec chaque message de manière à augmenter la probabilité selon laquelle chaque code DES produit par l'opération 1600 de production de code CA-DES sera unique. Dans la présente invention, la valeur du champ du code de session 240B et la valeur de la paire 5113D ("indice"), lorsqu'elles sont prises ensemble, seront normalement différentes pour chaque message de demande (c'est-à-dire le message CA1 et le message CA2) et chaque message de réponse (c'est-à-dire le message CA3 et le message CA4). De plus, la valeur de la paire 5113A ("type") fera la différence entre la demande et la réponse, se traduisant par une faible probabilité que deux messages quelconques soient cryptés avec le même code DES. Une variabilité supplémentaire est obtenue en utilisant la paire 5113B ("version").

Dans la présente invention, le chaînage de la valeur des paires 5113A, 5113B et 5113D du message CA1 se traduit par une quantité à quartet. Pour atteindre la valeur désirée des octets, le chaînage résultant est rempli sur le côté gauche avec des quartets de zéros.

A l'étape 1612, un vecteur d'initialisation à 64 bits est obtenu. Ce vecteur est les 64 bits inférieurs du code de session du champ 240B (figure 5E). Ce vecteur d'initialisation a été produit pendant l'opération 407 d'ouverture de session.

A l'étape 1613, une opération "OU Exclusif logique" est exécutée sur la quantité Q calculée à l'étape 1611 et le vecteur d'initialisation obtenu à l'étape 1612.

A l'étape 1614, le résultat de l'opération OU Exclusif de l'étape 1613 (valeur à 64 bits) est crypté en utilisant le code DES de 56 bits qui est stocké dans les 64 bits supérieurs du code-session du champ 240B. Le code DES de 56 bits a été produit pendant l'opération 407 d'ouverture de session.

A l'étape 1615, les bits de parité du résultat de l'opération OU Exclusif cryptée de l'étape 1614 sont détachés. De cette manière, le code DES de 56 bits, DES-CA1, est créé.

L'opération 1600 de production de code CA-DES pour le message CA1 se termine à l'étape 1617.

De nouveau en liaison avec la figure 27, l'opérataion CA12 d'assemblage de message pour le message CA1 se poursuit à l'étape 1625. Là, le DES-CA1 dans le code DES est stocké dans un registre temporaire.

A l'étape 1626, le logiciel d'application 210 du client accède à la structure 270 des données de grille de message (figure 5A) pour obtenir une liste de libellés, qui, lorsqu'ils sont adaptés aux valeurs associées, constituent les contenus de la section opaque du message CA1.

Les contenus de la section opaque du message CA1 sont représentés en figure 28B dans laquelle la paire 5117A comporte le libellé "montant". La valeur de la paire 5117A décrit la devise et le montant que l'utilisateur client 203 a l'intention de payer pour le produit.

La paire libellé-valeur 5117B comporte le libellé "code d'authentification" et est créée à l'étape 1628. Pour le message CA1, la valeur de la paire 5117B est un contrôle de total de somme du chaînage de ce qui suit : le sel à octet du champ 240C, les valeurs des pairs 5113A, 5113C-5113H, et 5117A et le sel à octet du champ 240C. Avant le contrôle de total de somme, la totalité de l'espace blanc compris dans les valeurs des paires 5113A, 5113C-5113H, et 5117A est enlevée et un caractère séparateur à barre verticale est inséré entre chaque paire adjacente de valeurs.

Ce code d'authentification n'est pas une signature numérique. Alors qu'une signature numérique pourrait être utilisée à la place du code d'authentification reflété dans la paire 5117B, le coût d'une telle utilisation en termes de temps de traitement

est important par rapport au traitement d'un contrôle de total de somme. Etant donné les sauvegardes fournies par l'utilisation de sessions indépendantes ayant une durée limitée pour le client utilisateur 203 et l'utilisateur commerçant 303, le bénéfice d'une non-répudiation sur la base d'un cryptage n'est pas suffisant pour contrebalancer le coût du temps de processeur.

A l'étape 1629, la paire libellé-valeur 5117B, créée à l'étape 1628, est annexée à la paire 5117A. Les paires 5117A et 5117B sont cryptées en utilisant le DES-CA1 en code DES qui est stocké dans le registre temporaire à l'étape 1625.

A l'étape 1630, la donnée cryptée à l'étape 1629 est codée en utilisant des techniques bien connues.

Le message CA1 est assemblé aux étapes 1631-1634. A l'étape 1631, l'en-tête 5105 est crée en utilisant la grille de message trouvée dans la structure 270 des données de grille de message-client (figure 5A) et le numéro de protocole tel qu'il est incorporé dans le logiciel d'application 210 du client.

A l'étape 1632, les paires libellé-valeur transparentes 5113A-5113H sont annexées.

A l'étape 1633, la paire libellé-valeur opaque 5117 est annexée. La paire 5117 comporte le libellé "opaque" signifiant que la valeur qui suit est une donnée cryptée. La valeur de la paire 5117 représente la donnée qui a été codée à l'étape 1630.

La queue 5150 est assemblée à l'étape 1634. Le total de contrôle de la queue 5150 est calculé comme on l'a décrit ci-dessus en ce qui concerne le message échantillon 4000. Le queue 5150 est ajoutée au reste du message CA1.

L'assemblage du message CA1 est maintenant terminé. L'opération d'assemblage de message CA12 pour le message CA1 se termine à l'étape 1635.

De nouveau en liaison avec la figure 24, le traitement se poursuit à l'étape 1707A. Là, l'ordinateur

200 du client ajoute un nouvel enregistrement 253 (figure 5I) de la façon suivante.

Le logiciel d'application 210 du client crée une valeur, de préférence, "paiement en espèces", et la sauvegarde dans le champ type 253A.

Le logiciel d'application du client crée également un numéro et une date de transaction et les stocke dans le champ de numéro de transaction 253B et le champ de date/heure 253C.

La version du logiciel d'application 210 du client utilisée pour créer le message CA1 est obtenue à partir du logiciel d'application 210 et est sauvegardée dans le champ de version de logiciel 253D.

Le numéro d'identification d'état civil pour l'état civil 120.1 du client est obtenu à partir du champ 220A et stocké dans le champ 253E.

La valeur de la paire libellé-valeur 5013C du message PR1 est sauvegardée dans le champ d'identification d'ordre 253F.

La valeur de la paire libellé-valeur 5113D est sauvegardée dans le champ 253G du numéro d'identification du commerçant.

La valeur associée à la paire libellé-valeur 5117A est sauvegardée dans le champ de montant 253H et est déduite du champ de valeur courante 240F de la structure 240 des données de session du client.

Le champ 253I du mémo d'utilisateur stocke une note facultative du client qui décrit la transaction. La valeur du champ 253I est obtenue à partir de l'utilisateur client 203 en réponse à une demande du logiciel d'application 210 du client au moment où l'utilisateur client 203 est d'accord pour procéder au paiement.

La valeur de la paire libellé-valeur 5013I du message PR1 est sauvegardée dans le champ 253J.

Une copie du message CA1 est de préférence sauvegardée dans le champ 253K.

De nouveau en liaison avec la figure 24, le traitement se poursuit à l'étape 1708. Là, l'ordinateur 200 du client transmet le message CA1 à l'ordinateur 300 du commerçant. L'ordinateur 200 du client attend un message de réponse CA4 de l'ordinateur 300 du commerçant.

A l'étape 1709, l'ordinateur 300 du commerçant reçoit le message CA1 en provenance de l'ordinateur 200 du client et dévoile le message CA1 en exécutant l'opération de dévoilement de message. L'opération pour le message CA1 sera maintenant décrite en liaison avec la figure 30, dans laquelle elle commence à l'étape 1641.

A l'étape 1642, le logiciel 310 du commerçant extrait le numéro de protocole de l'en-tête 5105 du message CA1. Ensuite, sur la base du numéro de protocole extrait du champ 5105C, la structure 380 des données de message est accédée pour déterminer le format attendu du message CA1. Le format attendu peut comprendre une syntaxe de message (par exemple caractères de fin de ligne permis) et le codage du message (par exemple ASCII ou hex). Le message CA1 est analysé en conformité avec le format attendu de la façon suivante.

A l'étape 1643, l'ordinateur 300 du commerçant calcule un total de contrôle en utilisant la même donnée qui a été utilisée par l'ordinateur 200 du client à l'étape 1633 l'opération CA12 d'assemblage de message (figure 27) pour le message CA1. A l'étape 1644, le total de contrôle calculé à l'étape 1643 est comparé au total de contrôle de la queue 5150 du message CA1. Si les totaux de contrôle ne sont pas égaux, le message CA1 est écarté à l'étape 1644B dans laquelle l'opération de dévoilement de message CA1 se termine.

Si les totaux de contrôle sont égaux à l'étape 1644, le traitement se poursuit à l'étape 1644B dans laquelle le message est vérifié pour déterminer s'il est approprié à l'opération CA1 de dévoilement de

message. Un message est approprié s'il comprend le libellé "type" dans la partie transparente du message et la valeur indiquant un message CA1. Si un message ne comprend pas cette paire libellé-valeur, il n'est pas approprié. Le message CA1 est approprié; par conséquent, le traitement se poursuit à l'étape 1645 dans laquelle une vérification de forme du message CA1 est effectuée.

L'opération de la vérification de forme de l'étape 1645 dépend de la version du logiciel. Plus précisément, la forme attendue du message, et les critères qui déterminent s'il est acceptable, dépendent du message et de toutes les variantes du message qui sont valables à un instant donné telles qu'elles sont déterminées par référence au type de message et à l'information sur la version qui sont fournies dans le message CA1 et par la structure 380 des données de message comme on l'a décrit précédemment. Au minimum, l'opération de vérification de forme établira si un message entrant contient tous les libellés qui sont prescrits pour ce message, s'il y a des valeurs de chaque libellé qui nécessitent une valeur, si les valeurs sont du type (par exemple texte, numéros signés), de la syntaxe et dans les limites spécifiées selon nécessité. Si un message ne peut être analysé, ou s'il peut être analysé mais ne satisfait pas les critères de forme, un indicateur d'erreur sera établi à l'étape 1647. Dans ce cas, l'opération CA1 de dévoilement de message se termine à l'étape 1648. Si le message CA1 passe la vérification de forme à l'étape 1645, le traitement se poursuit à l'étape 1646 dans laquelle la valeur de la paire 5117 est sauvegardée dans un registre temporaire. L'opération CA1 de dévoilement de message est terminé à l'étape 1648.

De nouveau en liaison avec la figure 24, le traitement reprend à l'étape 1710A. Si des indicateurs d'erreur ont été établis à l'étape 1647, le traitement se poursuit à l'étape 1710B dans laquelle les opérations de traitement des erreurs du commerçant sont appelées.

Si aucun indicateur n'a été établi à l'étape 1647, le traitement se poursuit à l'étape 1711A. Là, l'ordinateur 300 du commerçant assemble le message CA2 (figure 31) conformément à l'opération CA12 d'assemblage de message, représentée en figure 27. L'opération CA12 a été précédemment décrite pour le message CA1 avec l'exception suivante : le DES-CA2 en code DES est produit (au lieu du DES-CA1 en code DES) en utilisant l'opération 1600 du code CA-DES. Le contenu du message CA2 est le suivant.

La paire libellé-valeur 5213A comporte le libellé "type". La valeur de la paire 5213A se réfère à un enregistrement dans la structure 150 des données de message du serveur qui établit les libellés comprenant le message CA2. La valeur de la paire 5213A est obtenue à partir du logiciel d'application 310 du commerçant.

La paire libellé-valeur 5213B comporte le libellé "version" et se rapporte à un enregistrement relatif à l'enregistrement de type comme on l'a décrit ci-dessus. La valeur de la paire 5213B contient une information relative à la forme et au contenu des paires 5213A, 5213C, 5213D, et 5213E et une information pour décrypter et analyser les paires 5217.1 et 5217.2. Comme on le décrira ultérieurement, une information additionnelle relative à la forme et au contenu des paires 5217.1 et 5217.2 est fournie dans la paire libellé-valeur 5217.1B. La valeur de la paire 5213B est récupérée par le logiciel d'application 310 du commerçant à partir de la structure 380 des données de message (figure 6A).

La paire libellé-valeur 5213C comporte le libellé "numéro d'identification de session". La valeur de la paire 5213C est obtenue à partir du numéro d'identification de session du champ 340A (figure 6E).

La paire libellé-valeur 5213D comporte le libellé "indice". La valeur de la paire 5213D est un nombre entier affecté par le logiciel d'application 310 du commerçant à une transaction dans une session et

représente l'utilisation du code de session stocké dans le champ 240B.

La paire libellé-valeur 5213E comporte le libellé "catégorie de service". La valeur de la paire 5213E est un libellé qui peut être utilisé pour acheminer le message CA2 vers un processeur de l'ordinateur 100 du serveur qui traite les messages d'une catégorie de services particulière.

Le message CA2 comprend une paire libellé-valeur opaque de commerçant 5217.1 et une paire libellé-valeur opaque de client 5217.2. Les paires 5217.1 et 5217.2 comportent les libellés "commerçant-opaque" et "client-opaque", respectivement, signifiant que les valeurs qui suivent sont des données cryptées. La valeur de la paire 5217.1 représente la donnée qui était codée sur la base 64 à l'étape 1630. La valeur de la paire 5217.2 est la valeur de la paire 5117 (fournie par l'ordinateur 200 du client dans le message CA1) et sauvegardée dans le registre temporaire à l'étape 1646.

Les contenus de la section opaque du message CA2 sont représentés en figure 31B dans laquelle la paire libellé-valeur 5217.1A a le libellé "type". La valeur de la paire 5217.1A concerne un enregistrement dans la structure 150 des données de message qui établit les libellés des contenus de la section opaque du message CA2. La valeur de la paire 5217.1A est obtenue à partir du logiciel d'application 310 du commerçant.

La paire libellé-valeur 5217.1B comporte le libellé "version" et se rapporte à un enregistrement dans l'enregistrement "type" référencé par la paire 5217.1A. Comme on l'a décrit précédemment, la valeur de la paire 5217.1B permet à l'expéditeur d'un message d'aviser le destinataire du message quant à la version de ce message qui a été envoyée et d'indiquer au destinataire la façon d'analyser et de traiter cette version. La paire 5217.1B avise l'ordinateur 100 du serveur de la forme et du contenu de la paire libellé-valeur opaque 5217.1. La valeur de la paire 5217.1B est

obtenue à partir du logiciel d'application 310 du commerçant.

La présente invention permet de préférence à l'ordinateur 300 du commerçant de soumettre "n" messages CA1 qui proviennent d'un ou de plusieurs ordinateurs 200 de client à l'ordinateur 100 du serveur dans un seul message C2. Dans la présente invention, la variable "n" est un nombre entier compris entre 1 et 255. Une gamme différente pourrait être établie en fonction de la capacité du système et d'autres facteurs. Le message CA2 est structuré de façon que les paires libellé-valeur transparentes 5113A-5113D et 5113F-5113H d'un message reçu CA1 soient incluses dans la paire libellé-valeur opaque 5217.1. Pour chaque message CA2 soumis par l'ordinateur 300 du commerçant à l'ordinateur 100 du serveur, le message CA2 comprend les paires 5217.1C-5217.1I (correspondant aux paires 5113A-5113D et 5113F-5113H) et 5217.1J. Plus spécialement :

La paire libellé-valeur 5217.1C comporte le libellé "type-n" et la valeur de la paire 5117A.

La paire libellé-valeur 5217.1D comporte le libellé "sous version-n" et la valeur de la paire 5117B.

La paire libellé-valeur 5217.1E comporte le libellé "payeur-numéro d'identification-session-n" et la valeur de la paire 5117C.

La paire libellé-valeur 5217.1F comporte le libellé "payeur-indice-n" et la valeur de la paire 5117D.

La paire libellé-valeur 5217.1G comporte le libellé "note-contrôle de total de somme-n" et la valeur de la paire 5117F.

La paire libellé-valeur 5217.1H comporte le libellé "payeur-numéro d'identification-n" et la valeur de la paire 5117G.

La paire libellé-valeur 5217.1I comporte le libellé "ordre-numéro d'identification-n" et la valeur de la paire 5117H.

La paire libellé-valeur 5217.1J comporte le libellé "commerçant-montant-n". La valeur de la paire 5217.1J est fournie par le logiciel d'application 310 du commerçant et décrit la devise et le montant que l'utilisateur commerçant 303 s'attend à recevoir pour le produit.

De nouveau en liaison avec la figure 24, le traitement se poursuit à l'étape 1711B dans laquelle l'ordinateur 330 du commerçant met à jour ses structures de données locales de la façon suivante.

Un nouvel enregistrement 350.1 est créé dans la structure 350 des données de montant du commerçant pour les "n" messages CA1 inclus dans le message CA2. Le numéro d'identification d'ordre de la paire ordre-numéro d'identification-n est stocké dans le champ 350A. Le montant-commerçant de la paire commerçant-montant-n est stocké dans le champ 350B.

L'enregistrement 370.1 (figure 7C) est mis à jour de la façon suivante.

Le champ d'état 370B est établi à "tentative" par le logiciel d'application 310 du commerçant. Le numéro d'identification de session de l'utilisateur commerçant 303 provenant de la paire 5213C est stocké dans le champ 370G. L'indice de l'utilisateur commerçant 303 provenant de la paire 5213D est stocké dans le champ 370H. Le numéro d'identification de session de l'utilisateur client 203 de la paire 5217E est stocké dans le champ 370D. L'indice de l'utilisateur client 203 de la paire 5217F est stocké dans le champ 370E. La devise du commerçant est prélevée dans la valeur de symbole de devise dans la paire 5217J et sauvegardée dans le champ 370I. Le montant que le commerçant espère recevoir est prélevé dans la valeur de montant de la paire 5217K et est stocké dans le champ 370J.

De nouveau en liaison avec la figure 24, le traitement se poursuit à l'étape 1712. Là, l'ordinateur 300 du commerçant transmet le message CA2 à l'ordinateur

100 du serveur. L'ordinateur 300 attend un message de réponse CA3 de l'ordinateur 100.

A l'étape 1713.A, l'ordinateur 100 du serveur reçoit le message CA2 en provenance de l'ordinateur 300 du commerçant et sauvegarde une copie de la valeur de la paire 5213D du message CA2 dans le champ d'indice 130LL.1 (figure 4J) et une copie du message CA2 dans le champ 130LL.2. A l'étape 1713B, le serveur dévoile le message CA2 en exécutant l'opération 1660 de dévoilement de message du serveur. L'opération 1660 pour le message CA2 sera maintenant décrite en liaison avec les figures 32A et 32B, où elle commence à l'étape 1661.

A l'étape 1662, le logiciel 110 du serveur extrait le numéro de protocole du champ 5205C de l'en-tête 5205 du message CA2. Ensuite, sur la base du numéro de protocole extrait, la structure 150 des données de message est accédée pour déterminer le format attendu du message CA2. Le format attendu peut comprendre une syntaxe de message (par exemple caractères de fin de ligne permis), et le codage de message (par exemple ASCII ou hex). Le message CA2 est analysé en conformité avec le format attendu de la manière suivante.

A l'étape 1663, l'ordinateur 100 du serveur calcule un total de contrôle en utilisant la même donnée que celle utilisée par l'ordinateur 300 du commerçant à l'étape 1633 du mode opératoire CA12 d'assemblage de message pour le message CA2. A l'étape 1664, le total de contrôle calculé à l'étape 1663 est comparé au total de contrôle de la queue 5250 du message CA2. Si les totaux de contrôle ne sont pas égaux, le message CA2 est écarté à l'étape 1664A dans laquelle se termine l'opération 1660 de dévoilement du message du serveur.

Si les totaux de contrôle sont égaux à l'étape 1664, le traitement se poursuit à l'étape 1665A dans laquelle le message est vérifié pour déterminer s'il est approprié pour l'opération 1600 de dévoilement de message. Un message est approprié s'il comprend le

libellé "type" dans la partie transparente du message et la valeur indiquant un message CA2. Si le message ne comprend pas cette paire libellé-valeur, il n'est pas approprié et le traitement se poursuit à l'étape 1665C dans laquelle le message est dévié vers une autre opération de dévoilement qu'on décrit ailleurs. Le message CA2 est approprié; par conséquent, le traitement se poursuit à l'étape 1665C. Là, la valeur de la paire commerçant-libellé-valeur opaque 5217.1 est décodée.

A l'étape 1666, le logiciel 110 du serveur produit indépendamment le code DES-CA2, en code DES, indépendamment de l'ordinateur 300 du commerçant, en conformité avec le traitement 1600 de production de code CA-DES, qu'on a décrit précédemment.

A l'étape 1667, le code DES de 56 bits, DES-CA2, produit par l'ordinateur 100 du serveur est stocké dans un registre temporaire.

Le traitement se poursuit à l'étape 1668. Là, la paire libellé-valeur opaque du commerçant 5217.1 est décryptée en utilisant le code DES, DES-CA2.

A l'étape 1668A, le succès ou l'échec du décryptage de la paire 5217.1 est déterminé. Si le décryptage est un échec pour une raison quelconque, un indicateur d'erreur est établi à l'étape 1683 et l'opération 1660 de dévoilement de message de serveur se termine à l'étape 1682.

Si le décryptage est réussi, le traitement se poursuit à l'étape 1668B. Là, l'ordinateur 100 du serveur détermine si l'utilisateur commerçant 303 a une ouverture de session qui est valable. L'ordinateur 100 obtient le numéro d'identification de la session du commerçant à partir de la paire 5213C. Le numéro d'identification de session est utilisé pour obtenir l'enregistrement 130.2 du commerçant pour la session identifiée dans la paire 5213C. La date d'ouverture qui est stockée dans le champ 130GG est alors comparée à la date déterminée par référence à l'horloge de l'ordinateur 100 du serveur et le temps qui s'est écoulé

depuis la création de la session calculée. Si la valeur du temps qui s'est écoulé depuis la création de la session dépasse la valeur du champ durée de vie-code 130JJ, la session n'est pas valable. De plus, si la valeur dans la paire libellé-valeur d'indice 5213D dépasse la valeur de la limite d'utilisation de code qui est stockée dans le champ 130II, l'emploi de la session n'est pas valable. Si la session n'est pas valable, un indicateur de fermeture de session est établi à l'étape 1681 et l'opération de dévoilement CA2 se termine à l'étape 1682 et l'opération de paiement 1700 se poursuit à l'étape 1714.

Si la session est valable, à l'étape 1668C, le type de message est déterminé par référence à la paire libellé-valeur 5217.1A. Par exemple, la valeur de la paire 5217.1A pour le message CA2 peut être "collecte d'espèces".

Le traitement se poursuit à l'étape 1669. Là, l'ordinateur 100 du serveur exécute une vérification de la forme du message CA2. L'opération de vérification de forme de l'étape 1669 dépend de la version du logiciel. Plus précisément, la forme attendue du message, et les critères qui déterminent s'il est acceptable, dépendent du message et de toute variante du message qui sont valables à un instant donné tel que cela est déterminé par référence au type de message et à à la structure 150 de données de version comme on l'a décrit précédemment. Au minimum, l'opération de vérification de forme indiquera si un message entrant contient tous les libellés qui sont prescrits pour ce message, s'il y a des valeurs pour chaque libellé qui nécessitent une valeur, et si les valeurs sont du type (par exemple texte, nombres signés), syntaxe et dans toute limite spécifiée selon nécessité. Si un message peut être analysé mais ne remplit pas un critère de forme, l'ordinateur 100 du serveur établira un indicateur d'erreur à l'étape 1681 et renverra un code d'erreur dans le message CA3 qu'on décrit

ultérieurement. Dans ce cas, l'opération 6060 de dévoilement de message du serveur pour le message CA2 se termine à l'étape 1682.

Si le message CA2 passe la vérification de forme à l'étape 1669, le traitement se poursuit à l'étape 1670.

A l'étape 1670, le code d'authentification de l'utilisateur commerçant 303 représenté par la paire 5217.1K est vérifié de la façon suivante. Le logiciel 110 du serveur obtient le sel à octet du champ 130CC. Le logiciel 110 du serveur accède alors à la structure 150 des données de message pour déterminer les paires qui ont été l'objet d'un contrôle de total de somme à l'étape 1627 de l'opération CA12 d'assemblage du message CA2 pour calculer la valeur de la paire 5217.1K. Le logiciel 110 du serveur procède au contrôle de total de somme de ces mêmes paires libellé-valeur. Le sel à octet du champ 130CC est ajouté à la fois comme préfixe et comme suffixe des paires libellé-valeur avant le calcul du contrôle de total de somme. Cette valeur du contrôle est comparée à la valeur de la paire libellé-valeur 5217.1K. Si les valeurs sont différentes, un indicateur d'erreur approprié est établi à l'étape 1681. Dans ce cas, l'opération 1660 de dévoilement de message du serveur concernant le message CA2 se termine à l'étape 1682. Si les valeurs sont adaptées, le traitement se poursuit à l'étape 1671.

A l'étape 1671, la variable "n" est initialisée à un. La valeur de la variable "n", comme on l'a décrit ci-dessus, représente le $n^{ième}$ message CA1 inclus dans le message CA2.

A l'étape 1672, le logiciel 110 du serveur produit le DES-CA1 en code DES, conformément à l'opération 1600 de production de code DES-CA. Le DES-CA1 en code DES produit par l'ordinateur 100 du serveur est stocké dans un registre temporaire.

A l'étape 1673, la paire libellé-valeur opaque du client 5217.2 est décryptée en utilisant le CA1-DES en code DES.

A l'étape 1674, le succès ou l'échec du décryptage de la paire 5217.2 est déterminé. Si le décryptage est un échec pour une raison quelconque, un indicateur d'erreur est établi à l'étape 1678 et le traitement se poursuit à l'étape 1679. Là, on détermine s'il y a davantage de messages CA1 à traiter. Si tel est le cas, le traitement se poursuit à l'étape 1680. Dans le cas contraire, l'opération 1660 de dévoilement de message de serveur se termine à l'étape 1682.

Si le décryptage de la paire 5217.2 est réussi, le traitement se poursuit à l'étape 1675.

A l'étape 1675, le code d'authentification de l'utilisateur client 203 représenté par la paire libellé-valeur 5117B du message CA1 est vérifié de la façon suivante. Le logiciel 110 du serveur obtient le sel à octet du champ 130C. Le logiciel 110 du serveur accède alors à la structure 150 des données de message pour déterminer les paires libellé-valeur qui ont été l'objet d'un contrôle de total de somme à l'étape 1627 de l'opération CA12 d'assemblage pour le message CA1 afin de calculer la valeur de la paire 5117B. Le logiciel 110 du serveur procède au contrôle du total de somme de ces mêmes paires libellé-valeur. Le sel à octet du champ 130C est ajouté comme préfixe ainsi que comme suffixe aux paires libellé-valeur avant le calcul du contrôle de total de somme. Cette valeur du contrôle de total de somme est comparée à la valeur de la paire 5117B. Si les valeurs sont différentes, un indicateur d'erreur approprié est établi à l'étape 1678 et le traitement se poursuit à l'étape 1679. Là, on détermine s'il y a davantage de messages CA1 à traiter. Si ce n'est pas le cas, l'opération 1660 de dévoilement de message de serveur se termine à l'étape 1682. Si tel est le cas, le traitement se poursuit à l'étape 1680. Si les

valeurs sont adaptées à l'étape 1675, le traitement se poursuit à l'étape 1676.

A l'étape 1676, si le commerçant 303 a une session ouverte qui est valable, l'ordinateur 100 du serveur détermine si l'utilisateur client 203 associé à $n^{ième}$ demande de paiement incluse dans le message CA2 a une session ouverte qui est valable. L'ordinateur 100 obtient le numéro d'identification de session de l'utilisateur client 203 à partir de la paire libellé-valeur 5217.1E. Le numéro d'identification de session est utilisé pour obtenir l'enregistrement de session de client 130.1 pour la session identifiée dans la paire 5217.1E. La date d'ouverture stockée dans le champ 130G est alors comparée à la date qui est déterminée par référence à l'horloge de l'ordinateur 100 du serveur et au temps calculé qui s'est écoulé depuis la création de la session. La session n'est pas valable si le temps qui s'est écoulé depuis la création de la session dépasse la valeur du champ 130J de la durée de vie du code. La transaction n'est pas valable si la valeur de la paire libellé-valeur d'indice 5217.1F dépasse la valeur de la limite d'utilisation de code stockée dans le champ 130I. Si la session n'est pas valable, un indicateur de session fermée est établi à l'étape 1678 et le traitement se poursuit à l'étape 1679. Là, il est déterminé s'il y a davantage de messages CA1 à traiter. Si tel est le cas, le traitement se poursuit à l'étape 1680. Sinon, l'opération 1660 de dévoilement de message de serveur se termine à l'étape 1682.

Si la session de l'utilisateur client 203 est valable, le traitement se poursuit à l'étape 1667.

A l'étape 1677, le paiement à l'utilisateur commerçant 303 est effectué. Pour l'utilisateur client 203, cela signifie la déduction du montant reflété dans la paire libellé-valeur de montant 5217.2A du montant courant du champ 130F et la capture des données de transaction 130N de l'enregistrement 130.1. La donnée de transaction 130N est représentée en figure 4I dans

laquelle la donnée suivante est captée : le montant dans la paire 5217.2A est stocké dans le champ 13ON.1; le numéro d'identification de session du client provenant de la paire 5217.1E est stocké dans le champ 13ON.2; le numéro d'identification d'ordre de la paire 5217.1E est stocké dans le champ 13ON.3; le numéro d'identification de session de commerçant de la paire 5213C est stocké dans le champ 13ON.4; et l'indice de client de la paire 5217.1F est stocké dans le champ 13ON.5.

Pour l'utilisateur commerçant 303, ce paiement signifie l'addition du montant reflété dans le champ de montant 5117A au montant courant du champ 13OFF et la capture de la donnée de transaction 13ONN de l'enregistrement 130.2.130.1. La donnée de transaction 13ONN est représenté en figure 4K dans laquelle la donnée suivante est captée : le montant de la paire 5217.2A est stocké dans le champ 13ONN.1; le numéro d'identification de session du client de la paire 5217.1E est stocké dans le champ 13ONN.2; le numéro d'identification d'ordre de la paire 5217.1I est stocké dans le champ 13ONN.3; le numéro d'identification de session du commerçant de la paire 5213C est stocké dans le champ 13ONN.4; et l'indice de commerçant de la paire 5213D est stocké dans le champ 13ONN.5.

A l'étape 1679, le logiciel 110 du serveur détermine si le message CA2 comprend des messages CA1 additionnels à traiter. S'il y a des messages CA1 additionnels à traiter, la variable "n" est incrémentée à l'étape 1680 et le traitement se poursuit à l'étape 1672 comme on l'a décrit précédemment. S'il n'y a pas de messages CA1 additionnels à traiter, l'opération 1660 de dévoilement de message de serveur pour le message CA2 se termine à l'étape 1682.

Le traitement se poursuit à l'étape 1714 de la figure 24. Là, si des indicateurs d'erreur sont établis à l'étape 1681 à la suite des vérifications des étapes 1664, 1668A, 1668B, 1669 ou 1670, le traitement se poursuit à l'étape 1681. Là, le type d'erreur

provoquera l'association d'un code approprié à la paire libellé-valeur de code de réponse 5317.1C et l'association d'un message à la paire 5317.1E. Le niveau du détail détecté par les indicateurs d'erreur et reporté dans la paire libellé-valeur de code de réponse est une décision pour l'administrateur du système. Par exemple, un "échec" peut être un "échec de matériel", c'est-à-dire un échec d'un sous-ensemble d'échecs pour lequel une nouvelle soumission du message ne se traduira pas par le traitement du message (par exemple format non valable ou session fermée). Un "échec" peut aussi concerner un échec auquel il peut être remédié (un temps mort à cause d'un arrêt temporaire de l'ordinateur 100 du serveur). Dans la discussion qui suit, l'expression échec sera utilisée dans son sens large.

Si aucun indicateur n'a été établi à l'étape 1681, le traitement passe à l'étape 1716 dans laquelle l'ordinateur 100 du serveur détermine si les vérifications des étapes 1674, 1675 et 1676 des messages de demande de paiement ont provoqué l'établissement d'un indicateur d'erreur à l'étape 1678. Si le $n^{ième}$ message CA1 a provoqué l'établissement d'un indicateur, à l'étape 1717 la valeur de la paire 5317.1K (code de réponse-n) et la paire 5317.2A (code de réponse) seront établies comme échec; et la paire 5317.1N (problème-n) et la paire 5317.2E (problème) se verront affecter une valeur d'un code associé à la valeur de la paire 5317.1K. Si l'opérateur de l'ordinateur 100 du serveur considère que cela est souhaitable, un message en forme libre concernant l'échec sera inclus dans la paire 5317.1L (remarque-n) et la paire 5317.5A (remarque).

A l'étape 1718A, l'ordinateur 100 du serveur assemble le message CA3 conformément à l'opération 3400 d'assemblage de message du serveur, représentée en figure 33.

L'opération d'assemblage 3400 pour le message CA3 commence à l'étape 3401.

A l'étape 3402A, le logiciel 110 du serveur accède au type de message et à la structure 150 des données de version pour obtenir une liste de libellés, qui, lorsqu'ils sont adaptés à des valeurs associées, constituent les paires libellé-valeur transparentes 5313A-5313E pour le message CA3, représentées en figures 34A et 34B. A l'étape 3405A, des valeurs sont associées à chaque libellé de la façon suivante.

La paire libellé-valeur 5313A comporte le libellé "type". La valeur de la paire 5313A se rapporte à un enregistrement dans la structure 380 des données de message qui indique les libellés du message CA3. La valeur de la paire 5313A est obtenue à partir du logiciel 110 du serveur.

La paire libellé-valeur 5313B comporte le libellé "version" et se rapporte à un enregistrement relatif à l'enregistrement référencé par la paire 5313A. Comme on l'a discuté précédemment, la paire 5313B permet à l'expéditeur d'un message d'avertir le destinataire quant à la version de ce message et comment analyser et traiter cette version. Etant donné que le message CA3 est une réponse au message CA2 envoyé par l'ordinateur 300 du commerçant, la version du message CA3 sera sélectionnée par le logiciel 110 du serveur de façon à assurer qu'elle peut être traitée par le logiciel d'application 310 du commerçant. La paire 5313B indique au logiciel d'application 310 du commerçant la forme et le contenu des paires libellé-valeur transparentes 5313A, 5313C, 5313D et 5313E. La valeur de la paire 5313B est obtenue à partir du logiciel d'application 310 du commerçant.

La paire libellé-valeur comporte le libellé "numéro d'identification de session". La valeur de la paire 5313C est obtenue d'après le numéro d'identification de session du champ 130AA de la structure 130 des données de la session du commerçant.

La paire libellé-valeur 5313D comporte le libellé "indice". La valeur de la paire 5313D est

obtenue à partir de l'indice du champ 130LL de la structure 130.2 des données de session du commerçant.

La paire libellé-valeur 5313E comporte le libellé "catégorie de service". La valeur de la paire 5313E est un libellé qui peut être utilisé par l'ordinateur 300 du commerçant pour acheminer le message CA3 jusqu'à un processeur situé dans l'ordinateur 300 du commerçant qui traite les messages d'une catégorie de service particulière.

A l'étape 3402C, le logiciel 110 du serveur produit des codes DES de 56 bits, DES-CA3-C-n et DES-CA3-M. Les codes DES, DES-CA3-C-n et DES-CA3-M seront utilisés pour crypter les données devant être reçues par l'ordinateur 200 du client et l'ordinateur 300 du commerçant, respectivement. Les codes DES-CA3-C et DES-CA3-M sont produits conformément à l'opération 1600 de production de code CA-DES qu'on a décrite précédemment.

De nouveau en liaison avec la figure 33, une opération CA3 d'assemblage de message se poursuit à l'étape 3402D. Là, les codes DES, DES-CA3-C-n et DES-CA3-M sont stockés dans des registres temporaires.

A l'étape 3403, le logiciel 110 du serveur accède à la structure 150 des données de grille de message pour obtenir une liste de libellés, qui, lorsqu'ils sont adaptés à des valeurs associées, constituent les contenus de la section opaque du message CA3 (figure 34B). Des valeurs sont associées à chaque libellé de la façon suivante.

Les contenus de la section opaque-commerçant du message CA3 sont représentés en figure 34B où la paire 5317.1A comporte le libellé "sous-type". La valeur de la paire 5317.1A est un libellé se rapportant à un enregistrement dans la structure 380 des données de messages qui comprend les libellés des contenus de la section opaque-commerçant pour le message CA3. La valeur de la paire 5317.1A est obtenue à partir du logiciel 110 du serveur.

La paire libellé-valeur 5317.1B comporte le libellé "sous-version". La valeur de la paire 5317.1B est un code maintenu dans la structure 150 des données de message qui permet le traitement des variantes d'un type de message comme étant valable à un instant donné.

La paire libellé-valeur 5317.1C comporte le libellé "code de réponse" et la valeur "succès" ou "échec" comme on l'a décrit précédemment. La paire 5317.1C indique si la transaction présentée à l'ordinateur 100 du serveur par le message CA2 a été un succès, un échec, etc. La valeur de la paire 5317.1C est obtenue à l'étape 1715 décrite ci-dessus à partir du logiciel 110 du serveur.

La paire libellé-valeur 5317.1D comporte le libellé "honoraire". La valeur de la paire 5317.1D indique un honoraire chargé à l'utilisateur commerçant 303, s'il existe, associé au traitement du message CA2. La valeur de la paire 5317.1D est obtenue à partir du logiciel 110 du serveur.

La paire libellé-valeur 5317.1E comporte le libellé "problème". Si la valeur du code de réponse de la paire 5317.1C est autre que "succès", la valeur de la paire 5317.1E est un code indiquant à l'utilisateur commerçant 303 la cause de cette absence de succès. La valeur de la paire 5317.1E est obtenue à l'étape 1715 décrite ci-dessus à partir du logiciel 110 du serveur.

La paire libellé-valeur 5317.1F comporte le libellé "remarque". Si la valeur du code de réponse de la paire 5317.1C est autre qu'une valeur "succès", la valeur de la paire 5317.1F est un message de texte sous forme libre fournissant une explication détaillée de la raison de l'absence de succès. La valeur de la paire 5317.1F est obtenue à l'étape 1715 décrite ci-dessus à partir du logiciel 110 du serveur.

Le message CA3 comprend les paires libellé-valeur suivantes 5317.1G-5317.1P pour chacun des "n" messages CA1 soumis avec le message CA2 :

La paire libellé-valeur 5317.1G comporte le libellé "sous-type-n" et la valeur de la paire 5217.1C du message CA2.

La paire libellé-valeur 5317.1H comporte le libellé "sous-version-n" et la valeur de la paire 5217.1D du message CA2.

La paire libellé-valeur 5317.1I comporte le libellé "payeur-numéro d'identification de session-n" et la valeur de la paire 5217.1E du message CA2.

La paire libellé-valeur 5317.1J comporte le libellé "payeur-indice-n" et la valeur de la paire 5217.1F du message CA2.

La paire libellé-valeur 5317.1K comporte le libellé "réponse-code-n" et la valeur "succès" ou "échec" comme on l'a décrit précédemment. La valeur de la paire 5317.1K est obtenue à l'étape 1717 décrite ci-dessus à partir du logiciel 110 du serveur.

La paire libellé-valeur 5317.1L comporte le libellé "remarque-n". Si la valeur du code de réponse de la paire 5317.1K est autre qu'une valeur "succès", la valeur de la paire 5317.1L est un message de texte sous forme libre fournissant une explication détaillée de la raison de l'absence de succès. La valeur de la paire 5317.1L est obtenue à l'étape 1717 décrite ci-dessus à partir du logiciel 110 du serveur.

La paire libellé-valeur 5317.1M comporte le libellé "quantité collectée-n" et la valeur indiquant le montant des espèces électroniques collectées par l'utilisateur commerçant 303 pour la transaction (à l'étape 1677 de l'opération 1660 de dévoilement de message du serveur pour le message CA2).

La paire libellé-valeur 5317.1N comporte le libellé "problème-n". Si la valeur de la paire 5317.1K est autre qu'une valeur "succès", la valeur de la paire 5317.1N est un code indiquant à l'utilisateur client 203 la cause de l'absence de succès. La valeur de la paire 5317.1N est obtenue à l'étape 1717 décrite ci-dessus à partir du logiciel 110 du serveur.

La paire libellé-valeur 5317.1O comporte le libellé "numéro d'identification d'ordre-n". La valeur de la paire 5317.1O est obtenue à partir de la paire 5217.1I du message CA2.

La paire libellé-valeur 5317.1P comporte le libellé "demande-version". La valeur de la paire 5317.1P représente la version du message CA2 qui est actuellement traitée par l'ordinateur 1OO du serveur.

De nouveau en liaison avec la figure 33, à l'étape 3405, un code d'identification pour la section opaque-commerçant du message CA3, représentée par la paire 5317.1Q de la figure 34B, est créé. La paire 5317.1Q comporte le libellé "code d'authentification". La valeur de la paire 5317.1Q représente le code d'authentification de l'ordinateur 1OO du serveur. Pour la section opaque-commerçant du message CA3, la valeur de la paire 5317.1Q est un contrôle de total de somme MD5 du chaînage de ce qui suit : sel à octet du champ 13OCC, paires libellé-valeur 5313A-5313E et 5317.1A-5317.1P, et sel à octet du champ 13OCC. Avant le contrôle du total de somme, la totalité de l'espace blanc incorporé dans les paires 5313A-5313E et 5317.1A-5317.1P est enlevée.

A l'étape 3406, la paire libellé-valeur 5317.1Q, créée à l'étape 3405, est annexée aux paires 5317.1A-5317.1P. Les paires 5317.1A-5317.1Q sont cryptées en utilisant le code DES à 56 bits, DES-CA3-M.

A l'étape 3407, la donnée cryptée à l'étape 3406 est codée en utilisant des techniques bien connues.

A l'étape 3408, le logiciel 11O du serveur accède à la structure 15O des données de grille de message pour obtenir une liste de libellés, qui, lorsqu'ils sont adaptés aux valeurs associés, constituent les contenus de la section opaque-client du message CA3. Des valeurs sont associées à chaque libellé de la façon suivante.

Les contenus de la section opaque-client du message CA3 sont représentés en figure 34 dans laquelle

la paire 5317.2A comporte le libellé "code de réponse" et la valeur "succès" ou "échec". La paire 5317.2A indique si la transaction présentée à l'ordinateur 100 du serveur par le message CA2 a été un succès, un échec, etc. La valeur de la paire 5317.2A est obtenue à l'étape 1717 décrite ci-dessus à partir du logiciel 110 du serveur.

La paire libellé-valeur 5317.2B comporte le libellé "remarque". Si la valeur de code de réponse de la paire 5317.2A est autre qu'une valeur "succès", la valeur de la paire 5317.2B est un message en texte sous forme libre fournissant une explication détaillée de la raison de l'absence de succès. La valeur de la paire 5317.2B est obtenue à l'étape 1717 décrite ci-dessus à partir du logiciel 110 du serveur.

La paire libellé-valeur 5317.2C comporte le libellé "change étranger". La valeur de la paire 5317.2C fournit une information mise à jour qui concerne le taux de conversion de la dénomination de la devise incluse dans la valeur de la paire 5117A en d'autres devises. La valeur de la paire 5317.2C est obtenue à partir du logiciel 110 du serveur.

La paire libellé-valeur 5317.2D comporte le libellé "montant" et une valeur indiquant le montant des fonds chargés à l'utilisateur client 203 pour la transaction. La valeur de la paire 5317.2D est obtenue à partir du logiciel 110 du serveur.

La paire libellé-valeur 5317.2E comporte le libellé "problème". Si la valeur du code de réponse de la paire 5317.2A est autre qu'une valeur "succès", la valeur de la paire 5317.2E est un code indiquant à l'utilisateur client 203 la raison de l'absence de succès. La valeur de la paire 5317.2E est obtenue à l'étape 1717 décrite ci-dessus à partir du logiciel 110 du serveur.

La paire libellé-valeur 5317.2F comporte le libellé "numéro d'identification d'ordre". La valeur de

la paire 5317.2F est obtenue à partir de la paire 5217.1I du message CA2.

La paire libellé-valeur 5317.2G comporte le libellé "demande de version". La valeur de la paire 5317.2G représente la version du message CA1 actuellement traitée par l'ordinateur 100 du serveur.

De nouveau en liaison avec la figure 33, à l'étape 3410, un code d'authentification pour la section opaque-client du message CA3, représentée par la paire 5317.2H de la figure 34C, est créé. La paire 5317.2H comporte le libellé "code d'authentification". La valeur de la paire 5317.2H représentée en figure 34C indique le code d'authentification de l'ordinateur 100 du serveur. Pour la section opaque-client du message CA3, la valeur de la paire 5317.2H est un contrôle de total de somme d'un chaînage de ce qui suit : sel à octet du champ 130C, valeurs des paires 5313A-5313D et 5317.2A-5317.2G, et sel à octet du champ 130C. Avant le contrôle de total de somme, la totalité de l'espace blanc incorporé dans les valeurs des paires 5313A-5313D et 5317.2A-5317.2G est enlevée et un caractère de séparation à barre verticale est inséré entre chaque paire adjacente de valeurs.

A l'étape 3411, la paire libellé-valeur 5317.2H, créée à l'étape 3410, est annexée aux paires libellé-valeur 5317.2A-5317.2G. Les paires 5317.2A-5317.2H sont cryptées en utilisant le code DES, DES-CA3-C-n.

A l'étape 3412, la donnée cryptée à l'étape 3411 est codée en utilisant des techniques bien connues.

Le message CA3 est assemblé aux étapes 3413-3417. A l'étape 3413, l'en-tête 5305 est créé en utilisant la grille de messages trouvée dans la structure 150 des données de type et de version et le numéro de protocole tel qu'il est incorporé dans le logiciel 110 du serveur.

Ensuite, à l'étape 3414, les paires libellé-valeur transparentes 5313A-5313D sont ajoutées. Les paires 5313A-5313D ont été décrites précédemment.

Aux étapes 3415 et 3416, la paire libellé-valeur opaque-commerçant 5317.1 et la paire libellé-valeur opaque-client 5317.2 sont annexées. Les paires 5317.1 et 5317.2 ont les libellés "opaque-commerçant" et "opaque-client", respectivement, signifiant que les valeurs qui suivent sont des données cryptées. La valeur de la paire 5317.1 représente la donnée qui a été codée à l'étape 3407. La valeur de la paire 5317.2 représente la donnée qui a été codée à l'étape 3412 (qui sera acheminée jusqu'à l'ordinateur 200 du client dans le message CA4).

La queue 5350 est assemblée à l'étape 3417. Le total de contrôle de la queue 5350 est calculé comme on l'a décrit ci-dessus en ce qui concerne le message échantillon 4000. La queue 5350 est ajoutée au reste du message CA3.

L'assemblage du message CA3 est achevé. L'opération 3400 d'assemblage de message pour le message CA3 se termine à l'étape 3419.

A l'étape 1719, l'ordinateur 300 du commerçant reçoit le message CA3 en provenance de l'ordinateur 100 du serveur et dévoile le message CA3 en exécutant l'opération CA34 de dévoilement de message. L'opération CA34 concernant le message CA3 sera maintenant décrite en liaison avec la figure 35, qui commence à l'étape 2072.

A l'étape 2072, le logiciel 310 du commerçant extrait le numéro de protocole de l'en-tête 5305 du message CA3. Ensuite, sur la base du numéro de protocole extrait, la structure 380 des données de message est accédée pour déterminer le format attendu du message CA3. Le format attendu peut inclure une syntaxe de message (par exemple caractères de fin de ligne permis) et un codage de message (par exemple ASCII ou

hex). Le message CA3 est analysé en conformité avec le format attendu de la façon suivante.

A l'étape 2073, l'ordinateur 300 du commerçant calcule un total de contrôle en utilisant les mêmes données que celles utilisées par l'ordinateur 100 du serveur à l'étape 3417 de l'opération 3400 d'assemblage de messages pour le message CA3. A l'étape 2074, le total de contrôle calculé à l'étape 2073 est comparé au total de contrôle de la queue 5350 du message CA3. Si les totaux de contrôle ne sont pas égaux, le message CA3 est écarté à l'étape 2074A, dans laquelle se termine l'opération CA34 de dévoilement du message.

Si les totaux de contrôle sont égaux à l'étape 2074, le traitement se poursuit à l'étape 2075A dans laquelle le message est vérifié pour déterminer s'il est approprié pour l'opération CA34 de dévoilement de message. Un message est approprié s'il comprend le libellé "type" dans la partie transparente du message et la valeur indiquant un message CA3 ou CA4. Si un message ne comprend pas cette paire libellé-valeur, il est inapproprié. Le traitement d'un message inapproprié se produit à l'étape 2075B dans laquelle le message est dévié vers une autre opération de dévoilement qu'on décrit ailleurs. Le message CA3 est approprié; par conséquent, le traitement se poursuit à l'étape 2076 dans laquelle la valeur de la paire libellé-valeur opaque-commerçant 5317.1 est décodée.

A l'étape 2077, le logiciel d'application 310 du commerçant produit le même code DES, DES-CA3-M, produit par le logiciel 110 du serveur conformément à l'opération 1600 de production de code CA-DES.

A l'étape 2078, le code DES, DES-CA3-M, est stocké dans un registre temporaire.

A l'étape 2079, le code DES-CA3-M est utilisé pour décrypter la valeur de la paire libellé-valeur opaque-commerçant 5317.1.

Une vérification du message CA3 est alors exécutée à l'étape 2080 de la façon suivante.

A l'étape 2080, le succès ou l'échec du décryptage de la paire 5317.1 est déterminé. Si le décryptage est un échec pour une raison quelconque, un indicateur d'erreur est établi à l'étape 2084 et l'opération CA34 de dévoilement de message se termine à l'étape 2085.

Si le décryptage est réussi, à l'étape 2080A, le type de message est déterminé par référence à la paire 5317.1A. Par exemple, la valeur de la paire 5317.1A pour le message CA3 peut être "espèces-lot-réception".

Le traitement se poursuit à l'étape 2081. Là, l'ordinateur 300 du commerçant exécute une vérification de la forme du message CA3. L'opération de vérification de forme de l'étape 2081 dépend de la version du logiciel. Plus précisément, la forme attendue du message, et les critères qui déterminent s'il est acceptable, dépendent du message et des variantes du message qui sont valables à un instant donné comme cela est déterminé par référence à l'information sur le type et la version du message fournie dans le message CA3 et la structure 380 de la grille de message comme on l'a décrit précédemment. Au minimum, l'opération de vérification de forme indiquera si un message entrant contient tous les libellés qui sont prescrits pour ce message, s'il y a des valeurs pour chaque libellé qui nécessitent une valeur, et s'il y a des valeurs qui sont du type (par exemple texte, nombres signés), syntaxe et à l'intérieur de toute limite spécifiée selon nécessité. Si un message ne peut être analysé ou peut être analysé mais ne satisfait pas un critère de forme, l'ordinateur 300 du commerçant établira un indicateur d'erreur à une étape 2084 et l'opération CA34 de dévoilement de message se terminera à l'étape 2085.

Si le message CA3 passe la vérification de forme à l'étape 2081, le traitement se poursuit à l'étape 2082. Là, le code d'authentification représenté par la paire libellé-valeur 5317.1P est vérifié de la

façon suivante. Le logiciel 310 du commerçant obtient le sel à octet du champ 340C (figure 6E). Sur la base de la valeur de la paire libellé-valeur de sous-type 5317.1A et de la paire libellé-valeur de sous-version 5317.1B, le logiciel d'application 310 du commerçant accède alors à la structure 380 des données de grille de message afin de déterminer les paires libellé-valeur qui ont été l'objet d'un contrôle de total de somme à l'étape 3405 de l'opération CA3 d'assemblage de message afin de calculer la valeur de la paire 5317.1P. Le logiciel d'application 310 du commerçant ajoute alors le sel à octet du champ 340C comme préfixe ainsi que comme suffixe aux valeurs des mêmes paires libellé-valeur et calcule le contrôle de total de somme du résultat. Cette valeur du contrôle de total de somme est comparée à la valeur de la paire 5317.1Q. Si les valeurs sont différentes, un indicateur d'erreur approprié est établi à l'étape 2084. L'opération CA34 de dévoilement de message se termine à l'étape 2085.

De nouveau en liaison avec la figure 24, le traitement se poursuit à l'étape 1720. Là,

(1) si un indicateur d'erreur a été établi à l'étape 2084, il sera détecté à l'étape 1720 et le traitement du message CA3 se terminera à l'étape 1721.

(2) Si aucun indicateur d'erreur n'a été établi à l'étape 2084 mais qu'une erreur dans le message CA2 a été détectée à l'étape 1681, le traitement se poursuit à l'étape 1720B dans laquelle le contenu de la paire libellé-valeur 5317.1C est vérifié. Si la valeur de la paire 5317.1C est autre que "succès", les sous-programmes de traitement d'erreur sont exécutés à l'étape 1723, amenant le logiciel d'application 310 du commerçant à afficher le message contenu dans la valeur 5317.1F associée aux contenus de la valeur 5317.1C. Le logiciel d'application 310 du commerçant interprétera aussi la valeur de la paire 5317.1E et prendra toute action nécessaire qui peut être associée à cette valeur

et le traitement du message CA3 se termine à l'étape 1733; ou

(3) Si le message CA3 a passé la vérification à l'étape 1720 et à l'étape 1722, le traitement se poursuit à l'étape 1724 dans laquelle l'ordinateur 300 du commerçant met à jour la structure des données locales de la façon suivante.

L'enregistrement 350.1 (figure 3A) est mis à jour pour refléter si une demande de paiement a été payée. Le champ 350C contient un indicateur qui est établi soit à "payé", soit à "non-payé", en fonction du fait que le code réponse provenant de la paire 53217.1C est "succès" ou "échec". D'une façon similaire, l'enregistrement 370.1 (figure 7C) est mis à jour pour refléter l'état d'une demande de paiement particulière. Le champ 370B, qui est établi à "tentative" au moment d'une demande de paiement particulière, est envoyé à l'ordinateur 100 du serveur dans le message CA2, est établi à "succès" ou "échec" en fonction du fait que le code de réponse de la paire 5317.1C est "succès" ou "échec. Le code de résultat de la paire 5317.1E est stocké dans le champ 370M. L'honoraire payé par l'utilisateur commerçant 303 pour le traitement de la demande de paiement de la paire 5317.1D est stocké dans le champ 370L. Le montant recueilli par l'utilisateur commerçant 303 pour une demande de paiement particulière provenant de la paire 5317.1M est stocké dans le champ 370K et est ajouté au champ 360F de l'enregistrement 360.1 de la structure 360 des données de session de vente.

A l'étape 1725, l'ordinateur 300 du commerçant assemble le message CA4 conformément à l'opération 3100 d'assemblage de message, représentée en figure 36. Le message CA4 est représenté en figures 37A et 37B.

L'opération 3100 d'assemblage pour le message CA4 commence à l'étape 3101. A l'étape 3102, l'en-tête 5405 est créé en utilisant la grille de

message trouvée à la structure 380 des données de message et le numéro de protocole incorporé dans le logiciel d'application 310 du commerçant.

Ensuite, à l'étape 3103, les paires libellé-valeur transparentes 5413A-5413G sont ajoutées.

La paire libellé-valeur 5413A comporte le libellé "type". La valeur de la paire 5413A se rapporte à un enregistrement dans la structure 270 des données de message (figure 5A) qui indique les libellés du message CA4. La valeur de la paire 5413A est obtenue à partir du logiciel d'application 310 du commerçant.

La paire libellé-valeur 5413B comporte le libellé "version" et se rapporte à un enregistrement concernant un enregistrement référencé par la paire 5413A. Comme on l'a décrit précédemment, la paire libellé-valeur 5413B permet à l'expéditeur d'un message d'indiquer au destinataire la version de ce message, la façon de l'analyser et de traiter cette version. Comme le message CA4 est en réponse au message CA1 provenant de l'utilisateur client 203, la version utilisée par le logiciel d'application 310 du commerçant pour construire le message CA4 sera sélectionnée par le logiciel 310 pour avoir l'assurance qu'elle peut être traitée par le logiciel d'application 210 du client. La paire libellé-valeur 5313B indique au logiciel d'application 210 du client la forme et le contenu des paires libellé-valeur transparentes 5413A, 5413C et 5413D et de la paire libellé-valeur opaque 5417. La valeur de la paire 5413B est obtenue à partir du logiciel d'application 310 du commerçant.

La paire libellé-valeur 4313C comporte le libellé "session-numéro d'identification" et une valeur indiquant le numéro d'identification de session courante pour l'utilisateur client 203. L'ordinateur 300 du commerçant obtient la valeur de la paire libellé-valeur 5413C à partir de la valeur du numéro d'identification de session de la paire 5113C du message CA1.

La paire libellé-valeur 5413D comporte le libellé "indice". La valeur de la paire 5413D est un nombre entier choisi dans une gamme de valeurs non utilisées indiquant chaque fois qu'une transaction différente avec une session est tentée. L'utilisateur commerçant 303 obtient la valeur de la paire 5413D à partir de la valeur de l'indice de la paire 5113D du message CA1.

La paire libellé-valeur 5413F comporte le libellé "ordre-numéro d'identification". La valeur de la paire 5413F indique le numéro d'identification d'ordre produit par l'ordinateur 300 du commerçant pour identifier l'ordre. La valeur de la paire 5413F est la même que celle fournie dans la paire 5013C du message PR1.

La paire libellé-valeur 5413G comporte le libellé "catégorie de service". La valeur de la paire 5413G est un libellé qui peut être utilisé par l'ordinateur 100 du client pour acheminer un message CA4 jusqu'à un processeur de l'ordinateur 200 du client qui traite les messages d'une catégorie de service particulière.

A l'étape 3104, la paire libellé-valeur opaque 5417 est annexée. La paire 5417 comporte le libellé "opaque", signifiant que la valeur qui suit est une donnée cryptée. La valeur de la paire 5417 représente la valeur de la paire 5317.2, acheminée de l'ordinateur 100 du serveur jusqu'à l'ordinateur 300 du commerçant.

La queue 5450 est assemblée à l'étape 3105. Le total de contrôle de la queue 5450 est calculé comme on l'a décrit ci-dessus en ce qui concerne le message échantillon 4000. La queue 5450 est ajoutée au reste du message CA4.

L'assemblage du message CA4 est maintenant achevé. L'opération 3100 d'assemblage de message se termine à l'étape 3106.

De nouveau en liaison avec la figure 24, le traitement se poursuit à l'étape 1726. Là, l'ordinateur 300 du commerçant transmet le message CA4 à l'ordinateur 200 du client.

A l'étape 1727, l'ordinateur 200 du client reçoit le message CA4 en provenance de l'ordinateur 300 du commerçant et dévoile le message CA4 en exécutant l'opération CA34 de dévoilement de message. L'opération CA34 pour le message CA4 a été décrite précédemment pour le message CA3 en liaison avec la figure 35.

De nouveau en liaison avec la figure 24, le traitement se poursuit à l'étape 1728. Là,

(1) si un indicateur d'erreur a été établi à l'étape 2084, il sera détecté à l'étape 1728 et le traitement du message CA4 se terminera à l'étape 1729; ou

(2) si aucun indicateur d'erreur n'a été établi à l'étape 2084 mais qu'une erreur dans le message CA1 a été détectée à l'étape 1678, le traitement se poursuivra à l'étape 1730 dans laquelle le contenu de la paire libellé-valeur 5417A est vérifié. Si la valeur de la paire 5317A est autre que "succès", les sous-programmes de traitement d'erreur sont exécutés à l'étape 1731 amenant le logiciel d'application 210 du client à afficher le message contenu dans la paire 5417B qui est associée au contenu de la paire 5317.1C. Le logiciel d'application 210 du client interprétera aussi la valeur de la paire 5417E et prendra toute action qui peut être associée à cette valeur et le traitement du message CA4 se terminera à l'étape 1733; ou

(3) si le message CA4 a passé la vérification à l'étape 1728 et à l'étape 1730, le traitement se poursuit à l'étape 1732 dans laquelle l'ordinateur 200 du client met à jour sa structure de données de la façon suivante. L'ordinateur 200 compare la valeur contenue dans la paire 5417D à la valeur de la paire 5117A. Si les valeurs sont différentes, l'ordinateur 200 ajuste le champ du montant courant 240D

pour refléter le montant réellement déduit du champ du montant courant 130F tel qu'il est maintenu par l'ordinateur 100 du serveur. En plus des valeurs enregistrées dans la structure 240 des données de session du client, un nouvel enregistrement 263 de la structure 260 des données du journal du client est créé de la façon suivante. La date de la paire 5413E est stockée dans le champ 263C. Le code de réponse provenant de la paire 5417A est stocké dans le champ 263D. La remarque de la paire 5417B qui est associée au code de réponse de la paire 5417A est stockée dans le champ 263E. Le montant de la paire 5417D est stocké dans le champ 263J. Le N° d'identification d'ordre de la paire 5417F est stocké dans le champ 263G. Le numéro d'identification de session de la paire 5413C est stocké dans le champ 263L. L'indice de la paire 5413D est stocké dans le champ 263M.

G. Opération 411 de clôture de session.

L'opération 411 de clôture de session peut être utilisée par l'utilisateur client 203 pour fermer une session.

La figure 38 décrit un organigramme illustrant l'opération 411 qui commence à l'étape 1801.

A l'étape 1802, le logiciel d'application 210 du client indique à l'utilisateur client 203 d'entrer le numéro d'identification de la session à clore, toute note-enregistrement devant être jointe à une session, et le fait que l'utilisateur client 203 désire un journal des transactions soumises à l'ordinateur 100 du serveur par le commerçant 303 pour l'utilisateur client 203 pendant la session qui est en cours de clôture. Si l'utilisateur 203 a plusieurs sessions ouvertes, l'indication comprendra une liste de toutes les sessions ouvertes et demandera à l'utilisateur client 203 de choisir la session à clore.

Le contenu du message CS1 sera maintenant décrit en liaison avec les figures 39A et 39B.

La paire libellé-valeur 4813A comporte le libellé "numéro d'identification". La valeur de la paire 4813A indique le numéro d'identification d'état civil pour l'utilisateur client 203. La valeur de la paire 4813A est obtenue à partir du champ 220A (figure 5C).

La paire libellé-valeur 4813B comporte le libellé "transaction". La valeur de la paire 4813B est un numéro de transaction, produit par le logiciel d'application 210 de client, qui identifie de manière unique le message CS1. La valeur de la paire 4813B permet à l'ordinateur 100 du serveur, lors de la réception du message CS1, (1) d'envoyer un message de réponse associé CS2, décrit ci-dessous, et (2) de déterminer si le message CS1 est un message en duplication (c'est-à-dire déjà reçu par l'ordinateur 100 du serveur). La valeur associée à la paire 4813B est stockée dans le champ 256B.

La paire libellé-valeur 4813C comporte le libellé "date". La valeur de la paire 4813C indique la date et l'heure de l'assemblage du message CS1 et est envoyée à l'ordinateur 100 du serveur, conformément à l'horloge de l'ordinateur 200 du client. La valeur associée à la paire 4813C est stockée dans le champ 256C.

La paire libellé-valeur 4813D comporte le libellé "code de serveur". Comme on l'a décrit précédemment, la paire code DES/VI utilisée par l'ordinateur 200 du client pour crypter la paire opaque libellé-valeur 4817 du message CS1 est cryptée en utilisant le code public RSA de l'ordinateur 100 du serveur. La paire 4813D est dirigée vers le code privé RSA correspondant tel qu'il est stocké dans la structure 160 des données de code privé du serveur.

La paire libellé-valeur 4813E comporte le libellé "catégorie de service". La valeur de la paire 4813E est un libellé qui peut être utilisé dans

l'ordinateur 100 du serveur pour acheminer le message CS1 jusqu'à un processeur de l'ordinateur 100 du serveur qui traite les messages d'une catégorie de service particulière.

La paire libellé-valeur 4817 sera maintenant décrite. La paire libellé-valeur 4817 comprend le libellé "opaque" signifiant que la valeur qui suit est une donnée cryptée. La valeur de la paire 4817 représente la donnée qui a été codée à l'étape 813. Les contenus de la section opaque du message CS1 (figure 39B) sont les suivants :

La paire libellé-valeur 4817 comporte le libellé "type". La paire 4817A se rapporte à un enregistrement dans la structure 150 des données de message qui indique les libellés des contenus de la section opaque du message CS1. La valeur de la paire 4817A est obtenue à partir du logiciel d'application 210 du client qui produit le libellé lorsque l'utilisateur client 203 amorce une opération 411 de clôture de session.

La paire libellé-valeur 4817B comporte le libellé "date de serveur". La valeur de la paire 4817B indique la date et l'heure de l'assemblage du message CS1. Cette date et cette heure sont la perception par l'ordinateur 200 du client de l'horloge de l'ordinateur 100 du serveur.

La paire libellé-valeur 4817C comporte le libellé "version de logiciel". La valeur de la paire 4817C indique la version du logiciel d'application 210 du client qui communique avec l'ordinateur 100 du serveur et est obtenue à partir de la donnée incorporée dans le logiciel d'application 210. La valeur associée à la paire 5817C est également dans le champ 256D.

La paire libellé-valeur 4817D comporte le libellé "enregistrement-note". La valeur de la paire 4817D est une note au texte court facultative devant être stockée dans le champ 130M de la structure 130 des données de session du serveur concernant l'opération 411

de fermeture de session courante. La valeur de la paire 4817D est obtenue à partir de la réponse de l'utilisateur client 203 à une demande du logiciel d'application 210 du client et est de préférence limitée à soixante caractères pour la commodité de l'affichage. Si un enregistrement-note a été créé par l'utilisateur client 203 pendant l'opération 407 d'ouverture de session, la valeur de la paire 4817D est ajoutée à la valeur précédemment stockée dans le champ 130M.

La paire libellé-valeur 4817E comporte le libellé "session-numéro d'identification". La valeur associée à la paire 4817E est obtenue à partir du champ 240A de la structure 240 des données de session du client et est stockée dans le champ 256F.

La paire libellé-valeur 4817F comporte le libellé "demande-journal". La valeur associée à la paire 4817F est soit "oui" soit "non". La valeur de la paire 4817F reflète le fait que l'utilisateur-client 203 a ou non choisi de recevoir un journal des transactions à l'étape 1802. La valeur de la paire 4817F est stockée dans le champ 256G de la structure 250 des données en attente du client.

La paire libellé-valeur 4817G comporte le libellé "code". La valeur de la paire 4817H représente un contrôle de total de somme de la partie modulus de la paire code publié RSA/code privé pour l'état civil 120.1 du client. La valeur de la paire 4817G permet à l'ordinateur 100 du serveur de confirmer que le code public RSA conservé dans le champ 120B (figure 4B) est le même code que celui utilisé pour signer le message CS1. (paire 4817H).

La paire libellé-valeur 4817H comporte le libellé "signature". La valeur de la paire 4817I représente la signature numérique de l'état civil 120.1 du client. Pour le message CS1, la valeur de la paire 4817H est un contrôle de total de somme des paires 4813A-4813E et des paires 4817A-4817G dans l'ordre alphabétique, cryptées avec le code privé RSA de l'état

civil 120.1 du client. Le code privé RSA de l'état civil 120.1 est obtenu à partir du champ 220H.

A l'étape 1803, le message CS1 est assemblé en conformité avec l'opération 800 d'assemblage de message. L'opération 800 a été décrite précédemment pour le message R1 en liaison avec la figure 9. Une exception à noter : une copie du message CS1 est sauvegardée dans le champ 256H.

De nouveau en liaison avec la figure 38, l'opération 411 de clôture de session se poursuit à l'étape 1804. Là, l'ordinateur 200 du client transmet le message CS1 à l'ordinateur 100 du serveur. L'ordinateur 200 attend un message de réponse CS2 en provenance de l'ordinateur 100.

A l'étape 1805, l'ordinateur 100 du serveur reçoit le message CS1 en provenance de l'ordinateur 200 du client et dévoile le message CS1 en exécutant l'opération 900 de dévoilement de message de serveur pour le message CS1. L'opération 900 a été décrite précédemment par le message R1 en liaison avec la figure 11. Exception à noter : une copie du message CS1 est stockée dans le champ 140E.

A l'étape 1806, si l'un quelconque des tests des étapes 904, 909A, 912, 914, 1915 ou 916 a provoqué l'établissement d'un indicateur d'erreur à l'étape 905, les opérations de traitement des erreurs sont exécutées par l'ordinateur 100 du serveur à l'étape 1814. Alors que le niveau du traitement des erreurs à l'étape 1814 est largement une décision administrative, on préfère qu'au minimum, les défaillances de signature, et de forme, et un retour "fatal" de l'opération de vérification du logiciel se traduisent par un message de retour contenant un code qui peut être traité par le logiciel d'application 210 du client et par un message qui peut être lu par l'utilisateur client 203. L'opération de traitement des erreurs dans l'étape 1814 implique l'association d'un indicateur avec un code d'erreur spécifique (décrit dans le contexte du message

de retour CS2 ci-après) et la création d'un message de texte (soit à partir d'une structure de données de messages soit à partir d'un message envoyé par l'administrateur du système). L'ordinateur 100 du serveur produit alors un message CS2 similaire à celui décrit ci-dessus pour l'ordinateur 200 du client acheminant le code d'erreur et tout message concerné.

Si les tests des étapes 904, 909A, 912, 914, 915 et 916 n'ont pas provoqué d'établissement d'un indicateur d'erreur à l'étape 905, le traitement se poursuit à l'étape 1807. Là, l'ordinateur 100 du serveur invalide la session identifiée par la paire libellé-valeur 4817E en initialisant l'indicateur d'état dans le champ 130L comme étant "fermé".

A l'étape 1809, le logiciel 110 du serveur assemble le message de réponse CS2, conformément à l'opération 1000 d'assemblage de message du serveur. L'opération 1000 a été précédemment décrite pour le message R2 en liaison avec la figure 12. Le contenu du message CS2 (figures 40A et 40B) sera maintenant décrit.

La paire libellé-valeur 4913A comporte le libellé "numéro d'identification". La valeur de la paire 4913A indique le numéro d'identification de l'état civil pour l'utilisateur client 203. La valeur de la paire 4913A est obtenue à partir de la valeur de la paire 4813A du message CS1.

La paire libellé-valeur 4913B comporte le libellé "transaction". La valeur de la paire 4913B est un numéro de transaction. La valeur de la paire 4913B est la même que celle reçue dans le message CS1 dans la paire 4813B.

La paire libellé-valeur 4913C comporte le libellé "date". La paire 4913C a la même valeur que la paire 4813C du message CS1.

La paire libellé-valeur 4913D comporte le libellé "service-catégorie". La paire 4913D a la même valeur que la paire 4813E du message CS1.

Les contenus de la section opaque du message CS2 sont représentés en figure 49B dans laquelle la paire 4917A comporte le libellé "type". La valeur de la paire 4917A se rapporte à un enregistrement dans la structure 270 des données de message (figure 5A) qui établit les libellés des contenus de la section opaque du message CS2. La valeur de la paire 4917A est obtenue à partir du logiciel 110 du serveur.

La paire libellé-valeur 4917B comporte le libellé "serveur-date". La valeur de la paire 4917B indique la date et l'heure de l'assemblage du message CS2 conformément à l'horloge de l'ordinateur 100 du serveur.

La paire libellé-valeur 4917C comporte le libellé "réponse-code". La valeur de la paire 4917C indique si l'opération 411 de clôture de session a été un succès ou un échec.

La paire libellé-valeur 4917D comporte le libellé "sévérité du logiciel". La valeur de la paire 4917D indique si le logiciel d'application 210 du client a besoin d'être mis à jour, mais reste utilisable ("avertissement") ou n'est plus utilisable ("fatal"). La valeur de la paire 4917D est nulle si le logiciel d'application 210 du client est courant.

La paire libellé-valeur 4917E comporte le libellé "message de logiciel". La valeur de la paire 4917E donne des instructions sur ce que l'utilisateur client 203 doit faire dans le cas d'une sévérité du logiciel "fatal" ou "avertissement". La valeur de la paire 4917E n'est présente que si la valeur de la paire 4917D n'est pas nulle.

La paire libellé-valeur 4917F comporte le libellé "message". La valeur de la paire 4917F est un message en texte libre associé à une condition d'erreur ou de succès renvoyée dans la paire 4917C et est affichée pour l'utilisateur client 203.

La paire libellé-valeur 4917G comporte le libellé "honoraire". La valeur de la paire 4917G indique

un honoraire, s'il y en a un, chargé à l'utilisateur client 203 pour le traitement du message CS1.

La paire libellé-valeur 4917H comporte le libellé "montant" et indique le montant des fonds électroniques restant sur le montant alloué à la session pendant l'opération 407 d'ouverture de session après déduction de tous les paiements et honoraires. Si le traitement du message CS1 est réussi, le montant représenté par la paire 4917H sera ajouté au champ 120G.2 du conteneur d'espèces (figure 4C).

L'assemblage du message CS2 est maintenant terminé.

De nouveau en liaison avec la figure 38, à l'étape 1809A, le message CS2 est envoyé depuis l'ordinateur 100 du serveur à l'ordinateur 200 du client.

A l'étape 1810, l'ordinateur 200 du client reçoit le message CS2 en provenance de l'ordinateur 100 du serveur et dévoile le message CS2 en exécutant l'opération 1100 de dévoilement de message. L'opération 1100 pour le message CS2 a été décrite précédemment pour le message R2 en liaison avec la figure 14.

A l'étape 1811,

(1) Si un indicateur d'erreur a été établi à l'étape 1105, il sera détecté à l'étape 1811 et le traitement du message CS2 se terminera à l'étape 1812. Au point de vue de l'utilisateur client 203, aucune autre action n'est prise en ce qui concerne le message CS2. Dans la présente invention, un mécanisme est prévu dans le logiciel d'application 210 du client pour créer et envoyer un message à l'ordinateur 100 du serveur. Ce message comprend le message CS2 tel qu'il est reçu par l'ordinateur 200 du client et tout diagnostic sur ce qui a pu provoquer l'échec du message. Aucune réponse à ce message n'est envoyée par l'ordinateur 100 du serveur à l'ordinateur 200 du client. Au contraire, l'information est utilisée pour indiquer s'il existe un problème dans

le système et si des mesures de correction appropriées doivent être prises.

(2) Si aucun indicateur d'erreur n'a été établi à l'étape 1105 mais qu'une erreur dans le message CS1 a été détectée à l'étape 905, le traitement se poursuivra à l'étape 1813 dans laquelle le contenu de la paire 4717C est vérifié. Si la valeur de la paire 4917C est autre que "succès", les sous-programmes de traitement d'erreur sont exécutés à l'étape 1815, provoquant l'affichage par le logiciel d'application 210 du client du message contenu dans la paire 4917F associée au contenu de la paire 4917 et l'interprétation de la valeur de la paire 4917C et la prise de toute action qui peut être associée à cette valeur; ou

(3) Si le message CS1 a passé la vérification à l'étape 905 et que aucun indicateur n'a été établi à l'étape 1105, le traitement se poursuit à l'étape 1816 dans laquelle le logiciel d'application 210 du client met à jour la structure 202 des données de client de la façon suivante :

Le montant de la paire libellé-valeur 4917H est ajouté au champ 220J.

L'enregistrement 267 de la structure 260 des données du journal du client est mis à jour de la façon suivante : le numéro d'identification d'état civil de la paire 4913A est stocké dans le champ 267H. Le numéro de transaction de la paire 4913B est stocké dans le champ 267B. La date de la paire 4917B est stockée dans le champ 267C. Le code réponse de la paire 4917C est stocké dans le champ 267F. Le code de sévérité de logiciel de la paire 4917D est stocké dans le champ 267D. Le message de logiciel de la paire 4917E est stocké dans le champ 267E. Le message de réponse associé au code de réponse de la paire 4917F est stocké dans le champ 267G. L'honoraire de la paire 4917G est stocké dans le champ 267O. Le montant de la paire 4917H est stocké dans le champ 267I.

Si la valeur de la paire demande-libellé de journal-valeur 4817F dans le message CS1 a été établie à "oui", un rapport sera fourni à l'ordinateur 200 du client sur toutes les transactions amorcées par l'utilisateur client 203 pendant la session venant de se fermer.

Le traitement se poursuit à l'étape 1817 où l'opération 411 de clôture de session se termine.

V. Transaction d'échantillon.

On décrit ci-dessous une transaction d'échantillon. Dans cette transaction, l'utilisateur client 203 et l'utilisateur commerçant 303 exécutent chacun une opération d'inscription 401, une opération 403 de lien à un instrument financier, une opération 405 de chargement/déchargement, une opération 407 d'ouverture de session, une opération 409 de paiement d'une transaction, et une opération 411 de clôture de session. En exécutant ces opérations, l'utilisateur client 203 est à même d'acheter une paire de "chaussures rocket" provenant de Acme Products.

On remarquera que dans la présente invention, les paires libellé-valeur d'un message pour lesquelles aucune valeur n'a été affectée sont de préférence non incluses dans un message transmis. Cet attribut de la présente invention est reflété dans les messages échantillons décrits ci-dessous.

A. Opération 401 d'inscription.

L'opération 401 d'inscription est la même pour un client et un commerçant. Seule l'inscription de l'utilisateur client 203 est décrite ci-dessous.

L'utilisateur client 203 fait passer le logiciel d'application 210 du client qui indique à l'utilisateur client 203 son assentiment à un ou plusieurs accords légaux. En réponse à une demande

d'assentiment de l'utilisateur client 203 sur un accord légal, l'utilisateur client 203 choisit "accord". Le logiciel d'application 210 du client indique alors à l'utilisateur client 203 les informations suivantes : un numéro d'identification désiré d'état civil, l'adresse du protocole de transport du courrier de l'utilisateur client 203, le langage désiré dans lequel tout message d'erreur sera affiché, la phrase de passe d'auto-fermeture devant être associée à l'état civil, et la devise implicite de l'état civil.

En réponse à un message de guidage pour un numéro d'identification d'un état civil désiré, l'utilisateur client 203 choisit "brianb". En réponse à un message de guidage pour l'adresse du protocole de transport de courrier, l'utilisateur client 203 entre "brianb@reality.com". En réponse à un message de guidage pour le langage désiré pour le message d'erreur, l'utilisateur client 203 choisit "English" (anglais). En réponse à un message de guidage pour la phrase de passe d'auto-fermeture associée à l'état civil, l'utilisateur client 203 entre "badnews" (mauvaises nouvelles"). En réponse à un message de guidage pour la devise implicite de l'état civil, l'utilisateur choisit "dollars des Etats-Unis".

L'utilisateur client 203 est avisé d'entrer un mode de passe. L'utilisateur client 203 entre alors "entreprise". L'utilisateur 203 est avisé de re-entrer le mot de passe et se conforme. Le logiciel d'application 210 du client produit alors une paire code public RSA/code privé et initialise la création du message R1 comme on l'a décrit ci-dessus, message qui comprendra ce qui suit :

numéro de transaction :	2277052
date :	19951105100505456
code du serveur :	CC1001
type :	registration (inscription)
catégorie de service :	admin
opaque :	
date du serveur :	19951105100506656
version du logiciel :	1,Owin
langage du contenu :	en-us

devise implicite :	usd
numéro d'identification demandé :	BrianB
protocole de transport de courrier :	brianb@reality.com
accords :	75
phrase de passe d'auto-fermeture :	badnews (mauvaises nouvelles)
code public :	aslfflasdflasjylfdjslyafk jfjslakjfyldskajyflkajsyl dfjlaskfaslfjflasdflasjyk jfjslakjfjuyresdfutkpoiuq wasderfgthyujikolpkmn75cx zl
signature	sdjflsajflksjdlkfjlsakjfl kdsajflksjfjslakjfyldskaj yjfjslakjfyldskajydjlfasd loprytuazxcnmklokmnuhbvgy tfcdxszaqwe3r5t6y7u8iol09 km+

L'ordinateur 100 du serveur crée un nouvel enregistrement 140.1 dans le journal 140 des messages du serveur et sauvegarde une copie du message R1 dans le champ 140E. L'ordinateur 100 du serveur dévoile alors le message R1 et le traite comme on l'a décrit précédemment et met à jour l'enregistrement 140.1 du journal 140 des messages du serveur de la façon suivante :

numero d'identification d'état civil :	brianb-23
numéro d'identification de session	
numéro de transaction :	2277052
indice :	
message entrant :	copie du message R1
message de réponse :	

L'ordinateur 100 du serveur compare alors le numéro d'identification demandé par l'utilisateur client 203 à la liste des états civils existants. Si le numéro d'identification demandé est unique, il crée un enregistrement 120.1 d'état civil pour l'utilisateur client 203 de la façon suivante :

numéro d'identification d'état civil :	brianb-23
protocole de transport de courrier :	brianb@reality.com
code public :	aslfjflasdflasjylfdjslyaf kjfjslakjfyldskajyflkajsy ldfjlaskfaslfjflasdflasjy kjfjslakjfjuyresdfutkpoiu

	qwasderfgthyujikolpkmn75c xzl
date enregistrée :	19951105100507556
langage du contenu :	en-us
phrase de passe auto-fermeture :	badnews (mauvaises nouvelles)
donnée du conteneur d'espèces :	
accords :	
données de lien à un instrument :	

L'ordinateur 100 du serveur assemble alors le message R2, en sauvegarde une copie dans le champ 140 de l'enregistrement 140.1 de la structure 140 des données du journal de messages du serveur, et transmet le message R2 à l'ordinateur 200 du client. Le message R2 contient ce qui suit :

transaction :	2277052
date :	19951105100505456
type :	inscription-réponse
catégorie de service :	admin
opaque :	
date du serveur :	19951105100507556
numéro d'identification demandé :	brianb
numéro d'identification de réponse :	brianb-23
protocole de transport de courrier :	brianb@reality.com
code de réponse :	success (succès)
code public :	aslfjflasdflasjylfdjslyaf kjfjslakjfyldskajyflkajsy ldfjlaskfaslfjflasdflasjy kjfjslakjfjuyresdfutkpoiu qwasderfgthyujikolpkmn75c xzl
sévérité du logiciel :	warning (avertissement)
message du logiciel :	New software is available (nouveau logiciel disponible).

L'ordinateur 200 du client dévoile et traite le message R2 comme on l'a décrit précédemment. Le logiciel d'application 210 du client crée un enregistrement de l'état civil "brianb-23" dans la structure 220 des données d'état civil du client de la façon suivante :

numéro d'identification d'état civil :	brianb-23
protocole de transport de courrier :	brianb@reality.com
code public :	aslfjflasdflasjylfdjslyaf kjfjslakjfyldskajyflkajsy ldfjlaskfaslfjflasdflasjy kjfjslakjfjuyresdfutkpoiu qwasderfgthyujikolpkmn75c xzl
date enregistrée :	19951105100507556
langage du contenu :	en-us
phrase de passe d'auto-fermeture :	badnews (mauvaises nouvelles)
date du conteneur d'espèces:	
accords :	75
données de lien à un instrument :	
options du logiciel :	default (implicite)
code privé :	8ikuhbrfvedc3erfg56yu87yg Ookmsdfghjk3erfqwerty7yuh 8ij7yfgdcsdfv6y89iOolujmh ncvzx2wdplkjhgffdsawe/9+ 45rf6tg7yhkjhgf2waaz4ed5t gfv

B. Opération 403 de lien à un instrument financier.

L'opération 403 de lien à un instrument financier est la même tant pour les clients que pour les commerçants. Seul le lien d'un instrument par l'utilisateur client 203 sera décrit.

L'opération 403 de lien à un instrument commence lorsque l'utilisateur client 203 sélectionne l'opération de lien à un instrument à partir de l'application du client. Le logiciel d'application 210 du client indique à l'utilisateur client 203 un nom et une adresse implicites. L'utilisateur 203 entre alors "Brian Brian, 100 Elm Street, Nice Place, VA 00000 USA".

L'utilisateur client 203 sélectionne "compte bancaire" et est avisé des informations suivantes : numéro de compte bancaire; du fait que le compte bancaire est ou non le compte à auto-fermeture pour l'état civil; description du compte; et consentement de l'utilisateur client 203 à un ou plusieurs accords légaux. L'utilisateur 203 est avisé de changer toute

information nécessaire pour décrire le nom, l'adresse, le numéro de téléphone du détenteur de l'instrument.

En réponse à un message de guidage pour le numéro du compte bancaire, l'utilisateur client 203 entre "059013218175654". En réponse à un message de guidage, pour la réponse sur le fait que le compte est le compte à auto-fermeture pour l'état civil, l'utilisateur 203 entre "oui". En réponse à un message de guidage demandant le changement du nom, de l'adresse, et du numéro de téléphone affichés, l'utilisateur 203 refuse.

En réponse à un message de guidage pour une description du compte, l'utilisateur 203 entre "My fun account" ("Mon compte de distractions"). En réponse à un message de guidage sur le consentement de l'utilisateur 203 à un accord légal, le client choisit "agreed" (d'accord). L'utilisateur 203 est avisé de "faire le lien à un instrument" avec l'ordinateur 100 du serveur. Cet acte a pour effet que le logiciel d'application 210 du client crée un message BI1 comme on l'a décrit précédemment, message qui comprend ce qui suit :

numéro d'identification :	brianb-23
numéro de transaction :	2277053
date :	19951125100510589
code de serveur :	CC1001
catégorie de service :	admin
opaque :	
type :	bind-instrument (instrument lié)
date de serveur :	19951125100512689
version de logiciel :	1,0win
numéro d'instrument :	059013218175654
type d'instrument :	dda
catégorie d'instrument :	dda
fonctions d'instrument :	load, unload (chargement, déchargement)
sel d'instrument :	4bnm8poetqv=
nom d'instrument :	Brian Q. Brian
rue d'instrument :	100 Elm Street
ville d'instrument :	Nice Place
état d'instrument :	VA
code postal d'instrument:	00000
pays d'instrument :	USA
accords :	75,123
auto-fermeture :	yes (oui)
phrase de passe d'auto-fermeture :	badnews (mauvaises nouvelles)

code :	4/Roos+2ac8=
signature :	sjadlkaslzfzlksajzlffzlks ajzlffzlksajzlffzlksajzlf fzlksajzl ffzlksajzlfjszlfjsldfjlsk flsajfsa/9iu7hgfce/juy+po iuhnbvcdewqazxp

L'ordinateur du serveur crée un nouvel enregistrement 140.2 dans le journal 140 des messages du serveur et sauvegarde une copie du message BI1 dans le champ 140E. L'ordinateur 100 du serveur dévoile alors le message BI1 et le traite comme on l'a précédemment décrit et met à jour l'enregistrement 140.2 du journal 140 des messages du serveur de la façon suivante :

numéro d'identification d'état civil :	brianb-23
numéro d'identification de session :	
numéro de transaction :	2277053
indice :	
message entrant :	copy of BI1 (copie de BI1)
message de réponse :	

L'ordinateur 100 du serveur met alors à jour la structure 120.1 des données d'état civil du serveur pour l'état civil "brianb-23" en entrant "badnews" dans le champ 120F de la phrase de passe d'auto-fermeture et en ajoutant la date du lien de l'instrument au champ 120H de la façon suivante :

numéro d'identification d'état civil :	brianb-23
type d'instrument :	dda
numéro d'instrument :	aswerfevg [crypté]
devise indigène d'instrument :	usd
préfixe d'instrument :	055654
accords légaux :	75, 123
contrôle de total de somme d'instrument :	uou980y57rd98jnhgt54e3==
numéro d'identification d'émetteur :	735980
nom de détenteur d'instrument:	Ikpipoipoi [crypté]
adresse de détenteur d'instrument :	oipipoipipo [crypté]
date de lien d'instrument :	19951125100513583
date de première utilisation d'instrument :	
état du lien :	created (créé)
transaction de vente validée :	no (non)
limite de transaction de vente :	

transaction de crédit validée :	no (non)
limite de transaction de crédit :	
chargement d'espèces validé :	yes (oui)
limite de transaction du chargement d'espèces :	usd 1000.00 (1000,00 utilisés)
déchargement d'espèces validé:	yes (oui)
limite de transaction de déchargement d'espèces :	-1
lien d'auto-fermeture :	yes (oui)

L'ordinateur 100 du serveur assemble alors le message BI4, en sauvegarde une copie dans le champ 140F de l'enregistrement 140.2 du journal 140 des messages de serveur et envoie un message BI4 à l'utilisateur client 203. Le message BI4 contient ce qui suit :

numéro d'identification d'état civil :	brianb-23
numéro de transaction :	2277053
date :	19951125100510589
catégorie de service :	admin
opaque :	
type :	bind-instrument-response (réponse à lien d'instrument)
date de serveur :	19951125100513583
code de réponse :	succès (succès)
sévérité du logiciel :	warning (avertissement)
message du logiciel :	New software is available (nouveau logiciel disponible)
numéro d'instrument :	059013218175654
type d'instrument :	dda
émetteur d'instrument :	East Bak of the Mississippi
pays de l'émetteur d'instrument :	us
fonctions d'instrument :	load, unload (chargement, déchargement)
numéro d'instrument :	059013218175654
type d'instrument :	dda
émetteur d'instrument :	EastBank of the Mississippi
pays d'émetteur d'instrument :	us
fonctions d'instrument :	load, unload (chargement, déchargement)
sel d'instrument :	4bnm8poetqv=

L'ordinateur 200 du client dévoile le message BI4 et le traite comme on l'a décrit précédemment, puis met à jour l'enregistrement 220.1

dans la structure 220 des données d'état civil de client pour l'état civil "brianb-23" en ajoutant la donnée de lien de l'instrument au champ 220J comme suit :

numéro d'identification d'état civil :	brianb-23
numéro d'instrument :	059013218175654
description d'instrument :	my fun account
nom de détenteur :	Brian Brian
adresse de détenteur :	100 Elm Street
ville de détenteur :	Nice Place, VA
pays de détenteur :	USA
code postal de détenteur :	00000
code de pays de détenteur :	1
code de zone de détenteur :	703
téléphone de détenteur :	555-1212
devise :	usd
indicateur de transaction de vente :	no.(non)
indicateur de transaction de crédit :	no (non)
indicateur de déchargement de fonds :	yes (oui)
indicateur de chargement de fonds :	yes (oui)
état :	approved (agrée)
donnée récurrente d'instrument :	instrument-number: 059013218175654/instrument-type:dda/instrument-issuer:EastBankofthe Mississippi/instrument-issuer-country:us/instrument-functions:load,unload/instrument-salt:4bnm8poetqv=
accords :	75,123.

C. Opération 405 de chargement/déchargement.

L'opération 405 de chargement/déchargement commence au moment où l'utilisateur client 203 choisit l'opération de chargement à partir du logiciel d'application 210 du client. Le logiciel 210 indique à l'utilisateur client 203 l'instrument à partir duquel il y a lieu de charger des fonds à brianb-23 de l'état civil. L'utilisateur 203 choisit "my fun account" et est avisé du montant à transférer. En réponse à un message de guidage pour le montant, l'utilisateur 203 entre $100,00. Le logiciel d'application 210 du client assemble alors le message LU1 comme on l'a décrit

précédemment et l'envoie à l'ordinateur 100 du serveur. Le message LU1 contient les informations suivantes :

numéro d'identification :	brianb-23
numéro de transaction :	2277054
date :	19951105103517688
code du serveur :	CC1001
catégorie de service :	cash (espèces)
opaque :	
type :	load-unload-funds (chargement-déchargement de fonds)
date de serveur :	19951105103519788
montant :	usd 100.00
code :	4/Roos+2ac8=
signature :	11jwlrjwlimceiwlcefjdwewleiciwlcefjdwewleiciwlcefjdwewleicjwlierqiqhodqhoiwehqxq23jioerpoiuklhgrqwer7y6tghjuiko09p+po9ijht5re3wx

L'ordinateur du serveur crée un nouvel enregistrement 140.3 dans le journal 140 des messages du serveur et sauvegarde une copie du message LU1 dans le champ 140E. L'ordinateur 100 du serveur dévoile alors le message LU1 et le traite comme on l'a décrit précédemment et met à jour l'enregistrement 140.3 du journal 140 de la façon suivante :

numéro d'identification d'état civil :	brianb-23
numéro d'identification de session	
numéro de transaction :	2277054
indice :	
message entrant :	copy of LU1 (copie de LU1)
message de réponse :	

L'ordinateur 100 du serveur met alors à jour l'enregistrement 120.1 de l'état civil du client en ajoutant la donnée conteneur d'espèces au champ 120G comme suit :

devise :	usd
balance disponible :	100.00
balance en suspens :	0.00
numéro de compte d'agence :	113317834

L'ordinateur 100 du serveur assemble alors le message LU2, en sauvegarde une copie dans le champ 140E de l'enregistrement 140.3 du journal 140 des messages du serveur, et transmet le message LU2 à

l'ordinateur 100 du client. Le message LU2 contient les informations suivantes :

numéro d'identification :	brianb-23
numéro de transaction :	2277054
date :	19951105103517688
catégorie de service :	cash (comptant)
opaque :	
type :	load-unload-response (réponse à chargement) déchargement)
date de serveur :	19951105103607914
montant :	usd 100.00
code réponse :	success (succès)
message :	funds-loaded (fonds chargés)
sévérité du logiciel :	warning (avertissement)
message du logiciel :	New software is available (nouveau logiciel disponible)
honoraire :	usd 0.0
balance :	usd 100.00
fonds de la session :	usd 0.00
en suspens :	usd 0.00

L'ordinateur 200 du client dévoile le message LU2 et le traite comme on l'a décrit précédemment, puis met à jour l'enregistrement 220.1 dans la structure 220 des données d'état civil de client pour l'état civil "brianb-23" en entrant "usd 100" (dollars des Etats-Unis 100) dans le champ 220J du conteneur d'espèces.

D. Opération 407 d'ouverture de session.

L'opération 407 d'ouverture d'une session commence au moment où l'utilisateur client 203 choisit l'opération ouverture de session à partir du logiciel d'application 210 du client. Le logiciel d'application 203 du client indique alors à l'utilisateur client 203 les informations suivantes : durée de vie désirée de la session en minutes; nombre maximum de transactions à effectuer pendant la session; montant des fonds à mettre à dispositon pendant la session; et mémo décrivant la session.

En réponse à un message de guidage pour la durée de vie désirée de la session en minutes,

l'utilisateur client 203 entre "120". En réponse à un message de guidage pour le nombre maximum de transactions à effectuer pendant la session, l'utilisateur 203 entre "25". En réponse au message de guidage pour le montant des fonds à mettre à disposition pendant la session, le client entre "70,00". En réponse au message de guidage pour un mémo dérivant la session, l'utilisateur 203 entre "Christmas shopping spree" (bamboches pour achats de Noël).

Le client 200 assemble alors un message OS1 et l'envoie à l'ordinateur 100 du serveur. Le message OS1 comprend les informations suivantes :

numéro d'identification :	brianb-23
numéro de transaction :	2277055
date :	19951105104131914
code du serveur :	CC1001
catégorie de service :	cash (comptant)
opaque :	
type :	open-session (session ouverte)
date de serveur :	19951105104134014
version de logiciel :	1.0win
enregistrement-note :	Christmas shopping spree (bamboche pour achats de Noël)
montant :	usd 70.00
durée de vie de code :	0120
limite d'utilisation de code :	25
message :	4/Roos+2ac8=
signature :	kasdjflasjdz1kfuoi579384n g09kdfgj09eurtndfbnb909n1 ktujwjsi86tjf9086ptjfgr6j ir46edcloplaszxewqnym+09u hgtr432zxcvbhgrewql2rg8mk o01

L'ordinateur du serveur crée un nouvel enregistrement 140.4 dans le journal 140 des messages du serveur et sauvegarde une copie du message OS1 dans le champ 140E. L'ordinateur 100 du serveur dévoile alors le message OS1, le traite comme on l'a décrit précédemment et met à jour l'enregistrement 140.4 du journal 140 de la façon suivante :

numéro d'identification d'état civil :	brianb-23
numéro d'identification de session :	

numéro de transaction 2277055
indice :
message entrant : copy of OS1 (copie de OS1)
message de réponse :

L'ordinateur 100 du serveur crée alors un enregistrement 130.1 dans la structure 130 des données de session du serveur associée au numéro d'identification "brianb-23". L'enregistrement 130.1 contient les informations suivantes :

numéro d'identification de session : J/Pi+sqGtgH=
code de session : 7ujm8iktgTRrfv3edc9olk==
sel de session : aa5yh8fdkl+=
devise : usd
montant à l'ouverture : 70.00
montant courant : 70:00
date d'ouverture : 19951105104137179
date de fermeture :
limite d'utilisation de code : 15
durée de vie du code : 0060
numéro d'identification d'état civil : brainb-23
état : open (ouvert)
mémo : christmas shopping spree (bamboche pour achats de Noël)
date de transaction :

L'ordinateur 100 du serveur met également à jour l'enregistrement 120.1 dans la structure 120 des données d'état civil de serveur associée à "brianb-23" en déduisant le montant "70,00" du montant "100,00" du champ 120G.2 de la balance disponible du conteneur d'espèces qu'on a décrit précédemment. L'ordinateur du serveur assemble un message OS2, en sauvegarde une copie dans le champ 140F de l'enregistrement 140.4, et transmet le message OS2 à l'ordinateur 200 du client. Le message OS2 comprend les informations suivantes :

numéro d'identification : brianb-23
transaction : 2277055
date : 19951105104131914
catégorie de service : cash (comptant)
opaque :
    type : open-session-response (réponse à session ouverte)
    date de serveur : 19951105104137179
    code de réponse : success (succès)
    sévérité de logiciel : warning (avertissement)

message de logiciel :	New software is available (nouveau logiciel disponible)
durée de vie de code :	0060
limite d'utilisation de code :	15
montant :	usd 70.00
change étranger :	cad 0,60 gpb 1,55
fonds de session :	usd 70,00
balance :	usd 30,00
en suspens :	usd 0,00
honoraire :	usd 0,00
numéro d'identification de session :	J/Pi+sqGtgH=
code de session :	7ujm8iktgTRrfv3edc9olk==
sel de session :	aa5yh8fdkl+=

L'ordinateur 200 du client dévoile le message OS2 et le traite comme on l'a décrit précédemment, puis crée un nouvel enregistrement 240.1 dans la structure 240 des données de session du client qui est associée à "brianb-23" de la façon suivante :

numéro d'identification de session :	J/Pi+sqGtgH=
code de session :	7ujm8iktgTRrfv3edc9olk==
sel de session :	aa5yh8fdkl+=
devise :	usd
montant à l'ouverture :	70,00
montant courant :	70,00
date d'ouverture :	19951105104137179
limite d'utilisation de code :	15
durée de vie de code :	0060
mémo :	christmas shopping spr (bamboche pour achats de Noël).

L'opération par laquelle l'utilisateur commerçant 303 ouvre une session est la même, sauf qu'un commerçant ne transfèrera pas des fonds de son conteneur d'espèces à un registre de session. Cela est dû au fait qu'un commerçant s'attend à recevoir des fonds et n'a pas besoin des fonds mis à sa disposition pendant une session de vente. L'ordinateur 100 du serveur crée un enregistrement 130.2 dans la structure 140 des données de session du serveur qui est associée à "acme-12" de l'utilisateur commerçant 303 de la façon suivante :

numéro d'identification de session :	k/iL+tpPmHg=
code de session :	3ejkPOM7T+poBOW9ipqwZ8==
sel de session :	qw891k3vAZ==
devise :	usd

montant à l'ouverture :	0,00
montant courant :	0,00
date d'ouverture :	110595063012147
date de fermeture :	
limite d'utilisation de code :	090
durée de vie de code :	0960
numéro d'identification d'état civil :	acme-12
état :	open (ouvert)
mémo :	shoe department sales (ventes du département chaussures)
date de transaction :	

Lors de l'ouverture d'une session, l'ordinateur 303 du commerçant crée un nouvel enregistrement 370.1 dans la structure 310 des données du journal des espèces du commerçant de la façon suivante :

type :	open-session (session ouverte)
état :	open (ouvert-
numéro de transaction :	55443322
durée demandée de session :	0960
compte demandé de session :	90
numéro d'identification de session :	k/iL+tpPmHg=
code de résultat :	success (succès)

E. Opération 409 de paiement d'une transaction.

L'opération 409 de paiement d'une transaction commence au moment où l'utilisateur client 203 répond à une offre de l'utilisateur commerçant 303 de vendre des chaussures sous des termes spécifiés en choisissant un "paiement comptant" comme mécanisme de paiement. Cet acte a pour effet que l'ordinateur 300 du commerçant assemble le message PR1 et le transmet à l'ordinateur 200 du client comme on l'a décrit précédemment. Le message PR1 comprend les informations suivantes :

type :	payment-request (demande de paiement)
ccid de commerçant :	acme-12
numéro d'identification d'ordre de commerçant :	1231-3424-234242
date de commerçant :	19951105104536378

version de logiciel de commerçant :	foo69
note :	ACME Products Purchase of 1 pair "Rocket shoes" at $37,50 ea. Shipping and handling $5,00 Total Price: $42,50. Ship to : Achat d'une paire de "chaussure Rocket" à $37,50 pièce. Expédition et traitement $5,00 Prix total : $42,50 Expédié à : Brian Brian 100 Elm Street Nice Place, VA 00000 USA
montant de commerçant :	usd 42,50
montant 2 du commerçant :	cad 54,25
acceptations :	visa; master; amex; JCPenny; macy
RRU-payé à :	http;//www.ACME.com/Server payment
RRU-annulé :	http;//www.ACME.com/Cyber payment Cancel
RRU-succès :	http://www.ACME.com/order sucess
RRU-échec :	http;//www.ACME.com/orderfail
code de contrôle de total de somme signé du commerçant :	lSLzs/vFQ0BXfU98LZNWhQ==
contrôle de total de somme signé du commerçant :	klfjlkdfglkdfsutkdfjglds7503qwrtjtyuvnvidur09e58fdj9086jCS985kf9086kg9894j6g-rO94543jvndmkzazqpl

L'ordinateur 300 du commerçant crée aussi un nouvel enregistrement 350.1 de la structure 350 des données du montant de commerçant de la façon suivante :

numéro d'identification d'ordre :	1231-3424-234242
montant de la transaction :	usd 42,50
indicateur :	pending (en attente)

L'ordinateur 200 du client traite le message PR1 comme on l'a décrit précédemment. En réponse à un message de guidage provenant du logiciel d'application 210 du client, l'utilisateur client 203 indique son acceptation de l'offre de l'utilisateur commerçant 203 en choisissant "paiement comptant". Cet acte a pour

effet que l'ordinateur 200 du client assemble le message CA1 et le transmet à l'ordinateur 300 du commerçant. Le message CA1 comprend les informations suivantes :

type :	cash-payment (paiement comptant)
version :	1
numéro d'identification de session :	J/Pi+sqGtgH=
indice :	1
bénéficiaire-devise :	usd
note-contrôle de total de somme :	tyriokljhgbvxczm7rfde4==
bénéficiaire-numéro d'identification :	acme-12
ordre-numéro d'identification :	1231-3424-234242
catégorie de service :	cash (comptant)
opaque :	
montant :	usd 42,50
code d'authentification	iou234rfgvbmcqp+poliu7==

L'ordinateur 300 du commerçant traite le message CA1 comme on l'a décrit précédemment. L'ordinateur 300 assemble alors le message CA2 comme on l'a décrit précédemment et le transmet à l'ordinateur 100 du serveur. Le message CA2 comprend les informations suivantes :

version :	1
numéro d'identification de session:	k/iL+tpPmHg=
indice :	77
catégorie de service :	cash (comptant)
commerçant-opaque :	
type :	cash-collection (collecte d'espèces)
version :	1
$type_n$:	cash-payment (paiement comptant)
$sous\text{-}version_n$:	1
payeur-numéro $d'identification_n$ de session :	J/Pi+sqGtgH=
$payeur\text{-}indice_n$:	1
note-contrôle de $total\ de\ somme_n$:	kchfiZ5WAUlpkl/vlogwuQ==
bénéficiaire-numéro $d'identification_n$:	Acme-12
ordre-numéro $d'identification_n$:	1231-3424-234242
$commerçant\text{-}montant_n$:	usd 42,50
code d'authentification :	UjkHgtK/38uhzxs9io3/PL==

client-opaque :	jksyfditdfkjgdfut029jf9q0875jC Sjmgmbnfiur86fm9345kdkjrjghnvm fhazaplaksdijdfhjgutiroklop8tr ewqasz

L'ordinateur 300 du commerçant met à jour l'ordinateur 370.1 de la structure 370 des données du journal d'espèces du commerçant en ajoutant la donnée additionnelle suivante à l'enregistrement existant (la totalité de l'enregistrement 370.1 est représentée à des fins de clarté):

type :	cash payment (paiement comptant)
état :	pending (attente)
numéro d'identification d'ordre :	1231-3424-234242
client-numéro d'identification de session :	J/Pi+sqGtgH=
client-numéro d'indice :	1
client-devise :	usd
commerçant-numéro d'identification de session :	k/iL+tpPmHg=
commerçant-numéro d'indice :	77
commerçant-devise :	usd
commerçant-montant demandé :	42,50
montant crédité :	42,50
honoraires payés :	0,00
type :	open-session (session ouverte)
état :	open (ouvert)
numéro de transaction :	78765437
durée de session demandée :	0960
compte de session demandé :	90
numéro d'identification de session :	k/iL+tpPmHg=
résultat-code :	success (succès)

L'ordinateur du serveur crée un nouvel enregistrement 140.5 dans le journal 140 des messages de serveur et sauvegarde une copie de message CA2 dans le champ 140E. L'ordinateur 100 du serveur dévoile alors le message CA2, le traite comme on l'a décrit précédemment. L'ordinateur 100 vérifie les enregistrements 130.1 et 130.2 de la structure 130 des données de session du serveur pour déterminer si les états-civils brianb-23 et acme-12 ont des sessions ouvertes. Si une session n'est pas valable, l'ordinateur du seveur termine l'opération

409 de paiement de la transaction. Ici, l'ordinateur 100 du serveur traite et met à jour l'enregistrement 140.5 du journal 140 des messages du serveur de la façon suivante :

numéro d'identification d'état-civil :	acme-12
numéro d'identification de session :	k/iL+tpPmHg=
numéro de transaction : indice :	77
message entrant :	copy of message CA2 (copie du message CA2)
message de réponse :	

L'ordinateur du serveur met également à jour l'enregistrement 130.1 de la structure 130 des données de session de serveur en associant l'information suivante au champ 130N des données de transaction :

montant :	usd 42,50
client-numéro d'identification de session :	J/Pi+sqGtgH=
commerçant-numéro d'identification d'ordre :	1231-3424-234242
commerçant-numéro d'identification d'état civil :	acme-12
client-indice :	1

L'ordinateur du serveur met également à jour l'enregistrement 130.2 de la structure 130 des données de session du serveur en associant l'information suivante au champ 130NN des données de transaction :

montant :	usd 42,50
client-numéro d'identification de session :	J/Pi+sqGtgH=
commerçant-numéro d'identification d'ordre :	1231-3424-234242
commerçant-numéro d'identification d'état civil :	acme-12
commerçant-indice :	77

L'ordinateur 100 du serveur assemble alors le message CA3 et le transmet à l'ordinateur 300 du commerçant comme on l'a décrit précédemment. Le message CA3 comporte les informations suivantes :

type :	from-server (provenant du serveur)
version :	1
numéro d'identification de session :	k/iL+tpPmHg =
indice :	77
catégorie de service :	cash (comptant)

commerçant-opaque :	
sous-type :	cash-batch-receipt (espèces-réception de lot)
sous-version :	1
demande-version :	1
code de réponse :	success (succès)
honoraire :	usd 0,00
sous-type$_n$:	cash-payment-recept (espèces-réception de paiement)
sous-version$_n$:	1
payeur-numéro d'identification$_n$ de session :	J/Pi+sqGtgH=
payeur-indice$_n$:	1
réponse-code$_n$:	success (succès)
montant$_n$ collecté :	usd 42,50
ordre-numéro d'identification$_n$:	1231-3424-234242
code d'authentification :	p12P+/BNfr59dsXz+lmnTP==
client-opaque :	
catégorie de service :	cash (comptant)
code de réponse :	success (succès)
montant :	usd 42,50
numéro d'identification d'ordre :	1231-3424-234242
code d'authentification :	kjTUY7f7zr+pGB65RXE+hc==

L'ordinateur 300 du commerçant dévoile le message CA3 et le traite comme on l'a décrit précédemment. L'ordinateur 300 met à jour l'enregistrement 350.1 des structures 350 des données de montant du commerçant en mettant le champ d'indicateur 350C sur "payé".

L'ordinateur 300 met à jour l'enregistrement 370.1 de la structure 370 des données du journal d'espèces du commerçant de la façon suivante :

le champ d'état 370D est placé sur "succès". Le champ 370k du montant crédité est initialisé à "usd 42,50".

L'ordinateur du commerçant assemble le message CA4 et le transmet à l'ordinateur 200 du client. Le message CA4 comprend les informations suivantes :

type :	cash-payer-recept (espèces-payeur-réception)
version :	1
numéro d'identification de session :	k/iL+tpPmHg=
catégorie de service :	cash (comptant)
indice :	77

numéro d'identification d'ordre :	1231-3424-234242
opaque :	
code de réponse :	success (succès)
montant :	usd 42,50
numéro d'identification d'ordre :	1231-3424-234242
code d'authentification :	mhgD4QaBPkj+vWkjHytR5J==

L'ordinateur 200 du client dévoile et traite le message CA4 comme on l'a décrit précédemment. L'ordinateur 200 met à jour l'enregistrement 240.1 de la structure 240 des données de session de client en déduisant "$42,50" du champ 240F du montant courant, laissant une balance de $27,50.

F. Opération 411 de clôture de session.

L'opération 411 de clôture de sesion commence au moment où l'utilisateur client 203 choisit le message de guidage de clôture de session à partir de l'affichage sur l'ordinateur 200 du client. Cet acte a pour effet que l'ordinateur 200 assemble le message CS1 et le transmet à l'ordinateur 100 du serveur comme on l'a décrit précédemment. Le message CS1 comprend les informations suivantes :

numéro d'identification :	brianb-23
transaction :	2277056
date :	19951105110223666
code de serveur :	CC1001
catégorie de service :	cash (comptant)
opaque :	
type :	close-session (clôture-session)
date de serveur :	19951105110225766
version de logiciel :	1,0win
numéro d'identification de session :	J/Pi+sqGtgH=
journal demandé :	No (non)
code :	4/Roos+2ac8=
signature :	kasdjfzlskadufsodpirulksdnzlskd803dipodsifdfsadybmipjg4eazqer98jfejoiudfji98ytrnmvcxzaqw23rgtyhpmklolqazxsw34rfvgy+09okiju7yhnbg

L'ordinateur du serveur crée un nouvel enregistrement 140.6 dans le journal 140 des messages du

serveur et sauvegarde une copie du message CS1 dans le champ 140E. L'ordinateur 100 du serveur dévoile alors le message CS1, le traite comme on l'a décrit précédemment et met à jour l'enregistrement 140.6 de la façon suivante:

numéro d'identification d'état civil :	brianb-23
numéro d'identification de session :	
transaction :	2277057
indice :	
message entrant :	copy of CS1 (copie de CS1)
message-réponse :	

L'ordinateur 100 du serveur met alors à jour l'enregistrement 130.1 dans la structure 130 des données de session du serveur qui est associée au numéro d'identification d'état civil "brianb-23" en ajoutant la valeur du champ 130F du montant courant ($27,50) au montant du champ 120G.2 de la balance disponible du conteneur d'espèces qu'on a décrit précédemment pour une balance de $57,50, en entrant la valeur "19951105110301999" dans le champ 130H de la date de clôture, et en changeant le champ 130L d'état pour le faire passer de "ouvert" à "fermé".

L'ordinateur du serveur assemble un message CS2, en sauvegarde une copie dans le champ 140F de l'enregistrement 140.6, et transmet le message CS2 à l'ordinateur 200 du client. Le message CS2 comprend les informations suivantes :

numéro d'identification :	brianb-23
transaction :	2277057
date :	19951105110223666
catégorie de service :	cash (comptant)
opaque :	
type :	close-session-response (clôture de session-réponse)
date de serveur :	19951105110301999
code de réponse :	success (succès)
sévérité du logiciel :	warning (avertissement)
message de logiciel :	New software is available (nouveau logiciel disponible)
honoraires :	usd 0,00
montant :	usd 27,50

L'ordinateur 200 du client dévoile et traite le message CS2 comme on l'a décrit précédemment. L'ordinateur 200 met à jour le champ 220I de l'enregistrement 220.1 de la structure 220 des données d'état civil du client en ajoutant $27,50 à la valeur courante du champ 220I ($30,00) pour une balance de $57,50. L'ordinateur 200 annule l'enregistrement 240.1 de la structure 240 des données de session du client.

La présente invention n'est pas limitée aux exemples de réalisation qui viennent d'être décrits, elle est au contraire susceptible de modifications et de variantes qui apparaîtront à l'homme de l'art.

REVENDICATIONS

1 - Procédé pour une communication de sécurité dans un système de communication, dans lequel le système comprend un premier dispositif à l'emplacement d'un premier tiers, un second dispositif à l'emplacement d'un second tiers, et un serveur en communication avec eux, caractérisé en ce qu'il comprend :

(a) la création d'une première session associée au premier tiers, où la première session comporte des premiers paramètres d'utilisation pour limiter la durée pendant laquelle cette première session peut être utilisée et un premier ensemble de données, où les premiers paramètres d'utilisation et le premier ensemble de données peuvent être identifiés par le serveur;

(b) la création d'une seconde session associée au second tiers, où la seconde session comporte des seconds paramètres d'utilisation pour limiter la durée pendant laquelle cette seconde session peut être utilisée et un second ensemble de données, où les seconds paramètres d'utilisation et le second ensemble de données peuvent être identifiés par le serveur; et

(c) la liaison d'une portion de la première session avec une portion de la seconde session dans le système de communication, où la portion de cette première session comprend le premier ensemble de données et les premiers paramètres d'utilisation et la portion de la seconde session comporte le second ensemble de données et les seconds paramètres d'utilisation;

(d) la vérification des premier et second tiers sur la base d'au moins des portions des premier et second ensembles de données par le serveur; et

(e) la détermination du fait que les première et seconde sessions peuvent être utilisées sur la base des premiers et seconds paramètres d'utilisation pour le serveur,

de sorte que, lorsque le serveur vérifie les première et seconde tiers et détermine que les première et seconde sessions peuvent être utilisées, les premier et second tiers sont assurés d'une communication de sécurité dans le système de communication.

2 - Procédé selon la revendication 1, dans lequel certaines données du premier ensemble de données ne sont pas transmises entre le premier dispositif et le serveur après la création de la première session et certaines données du second ensemble de données ne sont pas transmises entre le second dispositif et le serveur après la création de la seconde session.

3 - Procédé selon la revendication 2, dans lequel les premier et second ensembles de données comprennent des premier et second codes respectivement, et dans lequel le serveur vérifie les premier et second tiers en utilisant les premier et second codes.

4 - Procédé selon la revendication 1, dans lequel les premiers paramètres d'utilisation sont déterminés par le premier tiers et les seconds paramètres d'utilisation sont déterminés par le second tiers.

5 - Procédé selon la revendication 1, dans lequel les premier et second paramètres d'utilisation sont déterminés par le serveur.

6 - Procédé selon la revendication 1, dans lequel les premiers paramètres d'utilisation comprennent (a) un montant des fonds électroniques mis à la disposition du premier tiers pendant la durée de la première session, (b) un laps de temps pendant lequel la première session durera et (c) un nombre de transactions que le premier tiers peut exécuter pendant la première session.

7 - Procédé selon la revendication 1, dans lequel les seconds paramètres d'utilisation comprennent (a) un laps de temps pendant lequel la seconde session durera et (b) un nombre de transactions que le second tiers peut exécuter pendant la seconde session.

8 - Procédé pour une communication de sécurité dans un système de communication, dans lequel le système de communication comporte un dispositif à l'emplacement d'un utilisateur et un serveur en communication avec lui, caractérisé en ce que le procédé comprend :

a. la transmission d'une demande depuis le dispositif au serveur pour créer une session à laquelle des paramètres d'utilisation sont associés;

b. le cryptage d'un premier code avec un second code par le serveur;

c. la transmission du premier code crypté et des paramètres d'utilisation associés à la première session depuis le serveur au dispositif;

d. la réception du premier code crypté et des paramètres d'utilisation par le dispositif et le décryptage du premier code crypté de façon que le dispositif puisse communiquer en sécurité dans le système de communication en employant le premier code décrypté conformément aux paramètres d'utilisation.

9 - Procédé selon la revendication 8, dans lequel le premier code est un codes DES.

10 - Procédé selon la revendication 9, dans lequel le second code est un code DES.

11 - Procédé selon la revendication 8, dans lequel la communication de sécurité s'effectue à un niveau de sécurité supérieur à celui du DES.

12 - Procédé selon la revendication 8, comprenant en outre un second dispositif à un second emplacement d'utilisateur où le second dispositif communique également avec le dispositif de l'utilisateur et le serveur, caractérisé en ce qu'il comprend en outre :

a. la transmission d'une seconde demande depuis le second dispositif au serveur afin de créer une seconde session à laquelle des seconds paramètres d'utilisation sont associés;

b. le cryptage d'un troisième code avec un quatrième code par le serveur;

c. la transmission du troisième code crypté et des seconds paramètres d'utilisation depuis le serveur au second dispositif;

d. la réception du troisième code crypté et des seconds paramètres d'utilisation par le second dispositif et le décryptage du troisième code de façon que le second dispositif puisse communiquer en sécurité dans le système de communication en utilisant le troisième code crypté conformément aux seconds paramètres d'utilisation.

13 - Procédé selon la revendication 12, dans lequel le troisième code est un code DES.

14 - Procédé selon la revendication 12, dans lequel le quatrième code est un code DES.

15 - Procédé selon la revendication 12, dans lequel la communication de sécurité s'effectue à un niveau de sécurité supérieur à celui du DES.

16 - Procédé selon la revendication 12, comprenant en outre :

a. la transmission d'un premier ensemble de données depuis le dispositif de l'utilisateur au second dispositif, où le premier ensemble de données comprend une portion cryptée et une portion non cryptée, où la portion cryptée est cryptée en utilisant le premier code décrypté et au moins une portion de la portion non cryptée du premier ensemble de données;

b. la réception du premier ensemble de données par le second dispositif et la transmission d'un second ensemble de données en même temps que la portion cryptée du premier ensemble de données entre le second dispositif et le serveur, où le second ensemble de données comprend une portion cryptée et une portion non cryptée, où la portion cryptée du second ensemble de données comporte au moins une portion de la portion non cryptée du premier ensemble de données, et où la portion

cryptée du second ensemble de données est cryptée en utilisant le troisième code décrypté et au moins une partie de la portion non cryptée du second ensemble de données; et

c. la réception du second ensemble de données transmis à partir du second dispositif par le serveur et le décryptage de la portion cryptée du second ensemble de données en utilisant le troisième code et la partie de la portion non cryptée du second ensemble de données de sorte que la portion du premier ensemble de données incluse dans la portion cryptée du second ensemble de données est décryptée, et le décryptage de la portion cryptée du premier ensemble de données en utilisant le premier code et la partie de la portion décryptée du premier ensemble de données,

de sorte que l'utilisateur est vérifié par le serveur en utilisant le premier code et le second utilisateur l'est par le serveur en utilisant le troisième code.

17 - Système de transfert électronique dans un réseau de communication pour traiter une transaction entre un client ayant un dispositif de client, et un commerçant ayant un dispositif de commerçant, et un serveur qui leur sont connectés, où la transaction comporte des termes qui leur sont associés et où le serveur transfère des fonds électroniques entre le client et le commerçant de façon que le commerçant puisse fournir un produit au client, caractérisé en ce qu'il comprend :

a. le dispositif du commerçant pour :

(1) obtenir une première session de la part du serveur,

(2) transmettre une facture comprenant au moins une portion des termes de la transaction au dispositif du client,

(3) recevoir une réponse du client à la facture à partir du dispositif du client et transmettre un premier ensemble de données représentant

la transaction au serveur, où le premier ensemble de données comprenant au moins une portion de la réponse du client,

(4) recevoir un second ensemble de données en provenance du serveur indiquant si la transaction a été approuvée par le serveur, où le second ensemble de données comprend une partie commerçant et une partie client, où la partie commerçant et la partie client du second ensemble de données comprennent au moins une portion du premier ensemble de données; et

(5) transmettre la partie client du second ensemble de données au dispositif du client;

(b) le dispositif du client pour

(1) obtenir une seconde session de la part du serveur,

(2) recevoir la facture comportant la portion des termes de la transaction depuis le dispositif du commerçant et transmettre la partie de la réponse du client au dispositif du commerçant, et

(3) recevoir la partie client du second ensemble de données depuis le dispositif du commerçant;

(c) le serveur ayant un état civil de commerçant et un état civil de client qui y sont stockés, où l'état civil du commerçant représente le commerçant et l'état civil du client représente le client, où l'état civil du commerçant comporte une structure de stockage de fonds électroniques du commerçant qui lui est associée pour stocker des fonds électroniques reçus par le commerçant et l'état civil du client comporte une structure de stockage de fonds électroniques du client qui lui est associée afin de stocker des fonds électroniques du client, où le serveur sert à

(1) fournir la première session au dispositif du commerçant et la seconde session au dispositif du client,

(2) recevoir le premier ensemble de données représentant la transaction à partir du dispositif du commerçant et traiter le premier ensemble de données afin de déterminer si la transaction a été approuvée,

(3) transférer les fonds électroniques à partir de la structure de stockage des fonds électroniques du client à la structure de stockage des fonds électroniques du commerçant si la transaction a été approuvée, et

(4) transmettre le second ensemble de données au dispositif du commerçant, indiquant si la transaction a été approuvée,

de sorte que si la transaction a été approuvée, le commerçant peut fournir le produit au client.

18 - Système de transfert électronique selon la revendication 17, dans lequel le dispositif du commerçant comprend en outre la communication avec le serveur afin de lier un premier instrument financier à l'état civil du commerçant; et

où le dispositif du client comprend en outre la communication avec le serveur pour lier un second instrument financier à l'état civil du client.

19 - Système de transfert électronique selon la revendication 18, dans lequel le dispositif du client comprend en outre la transmission d'une demande au serveur afin de transférer des fonds du second instrument financier à la structure de stockage des fonds électroniques du client; et

où le serveur comporte en outre la réception et le traitement de la demande de transfert des fonds, afin de transférer des fonds du second instrument financier à la structure de stockage des fonds électroniques du client.

20 - Système de transfert électronique selon la revendication 19, dans lequel le dispositif du client comprend un conteneur de session de client pour stocker

des fonds électroniques du client pendant la seconde session, et comporte en outre la transmission d'une seconde demande au serveur afin de transférer des fonds électroniques depuis la structure de stockage de fonds électroniques du client au conteneur de session du client; et

où le serveur comporte en outre le traitement de la seconde demande et le transfert des fonds électroniques depuis la structure de stockage des fonds électroniques du client au conteneur de session du client.

21 - Système de transfert électronique selon la revendication 20, dans lequel l'utilisation de la première session est limitée par des premiers paramètres d'utilisation comportant (a) le laps de temps pendant lequel la première session peut durer et (b) le nombre de transactions que le commerçant peut exécuter pendant la première session; et

où l'utilisation de la seconde session est limitée par des seconds paramètres d'utilisation comprenant (a) un montant des espèces électroniques mises à la disposition du client pendant la seconde session, (b) le laps de temps pendant lequel la seconde session peut durer et (c) le nombre des transactions que le client peut exécuter pendant la seconde session.

22 - Système de transfert électronique selon la revendication 21, dans lequel le dispositif du commerçant comporte en outre la transmission d'une troisième demande pour transférer des fonds électroniques depuis le conteneur de session du commerçant à la structure de stockage des fonds électroniques du commerçant; et

où le dispositif du client comprend en outre la transmission d'une quatrième demande pour transférer des fonds électroniques depuis le conteneur de session du client à la structure de stockage des fonds électroniques du client; et

le serveur comporte en outre le traitement de la troisième demande afin de transférer les fonds électroniques depuis le conteneur de session du commerçant à la structure de stockage de fonds électroniques du commerçant et pour traiter la quatrième demande et pour transférer les fonds électroniques depuis le conteneur de session du client à la structure de stockage de fonds électroniques du client.

23 - Système de transfert électronique selon la revendication 21, dans lequel le serveur comprend en outre :

le transfert de fonds électroniques depuis le conteneur de session du commerçant à la structure de stockage de fonds électroniques du commerçant lorsqu'au moins l'un des premiers paramètres d'utilisation est satisfait; et

le transfert de fonds électroniques depuis le conteneur de session du client à la structure de stockage de fonds électroniques du client quant au moins l'un des seconds paramètres d'utilisation est satisfait.

24 - Système de transfert électronique selon la revendication 22, dans lequel le serveur comporte en outre la cessation des première et seconde sessions lorsqu'au moins l'un des premiers et seconds paramètres d'utilisation a été satisfait.

25 - Système de transfert électronique selon la revendication 23, dans lequel le dispositif du commerçant comprend en outre la transmission d'une cinquième demande au serveur afin de transférer des fonds en espèces électroniques depuis la structure de stockage de fonds électroniques du commerçant au premier instrument financier; et

le serveur pour le traitement de la cinquième demande et pour transférer des fonds électroniques depuis la structure de stockage de fonds électroniques du commerçant au premier instrument financier.

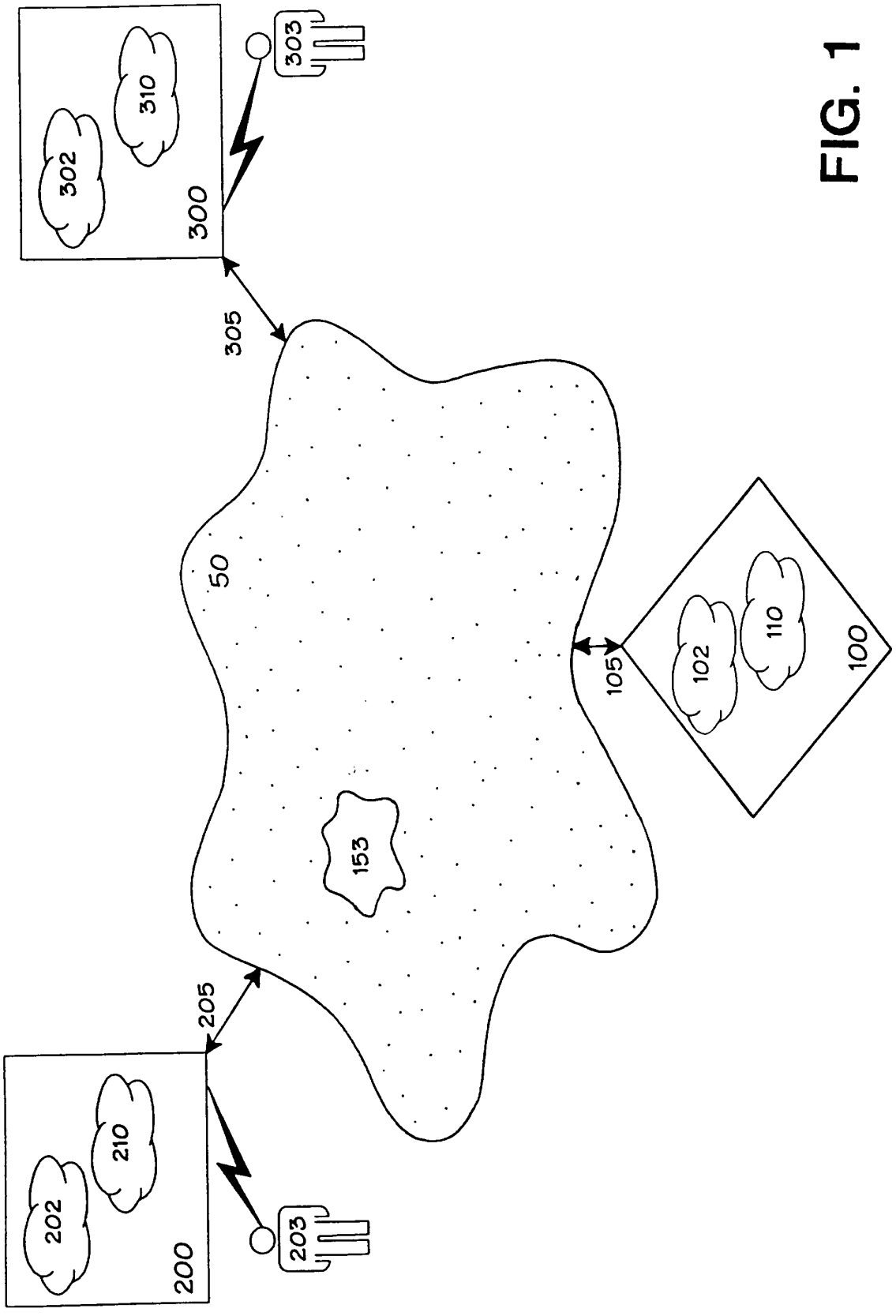
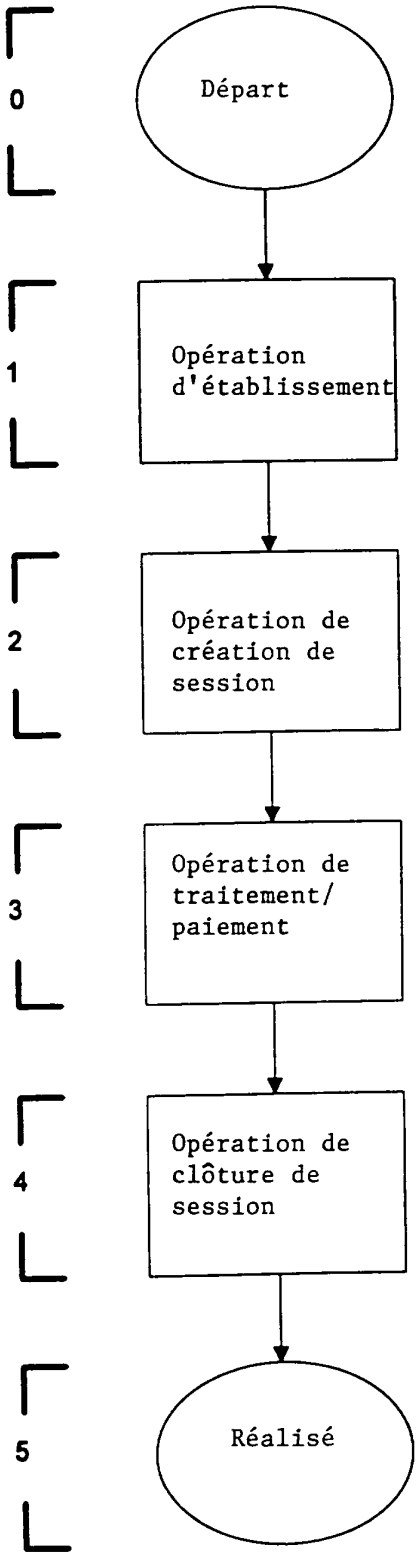


FIG. 1

FIG. 2


0
Départ
1
Opération d'établissement
2
Opération de création de session
3
Opération de traitement/ paiement
4
Opération de clôture de session
5
Réalisé

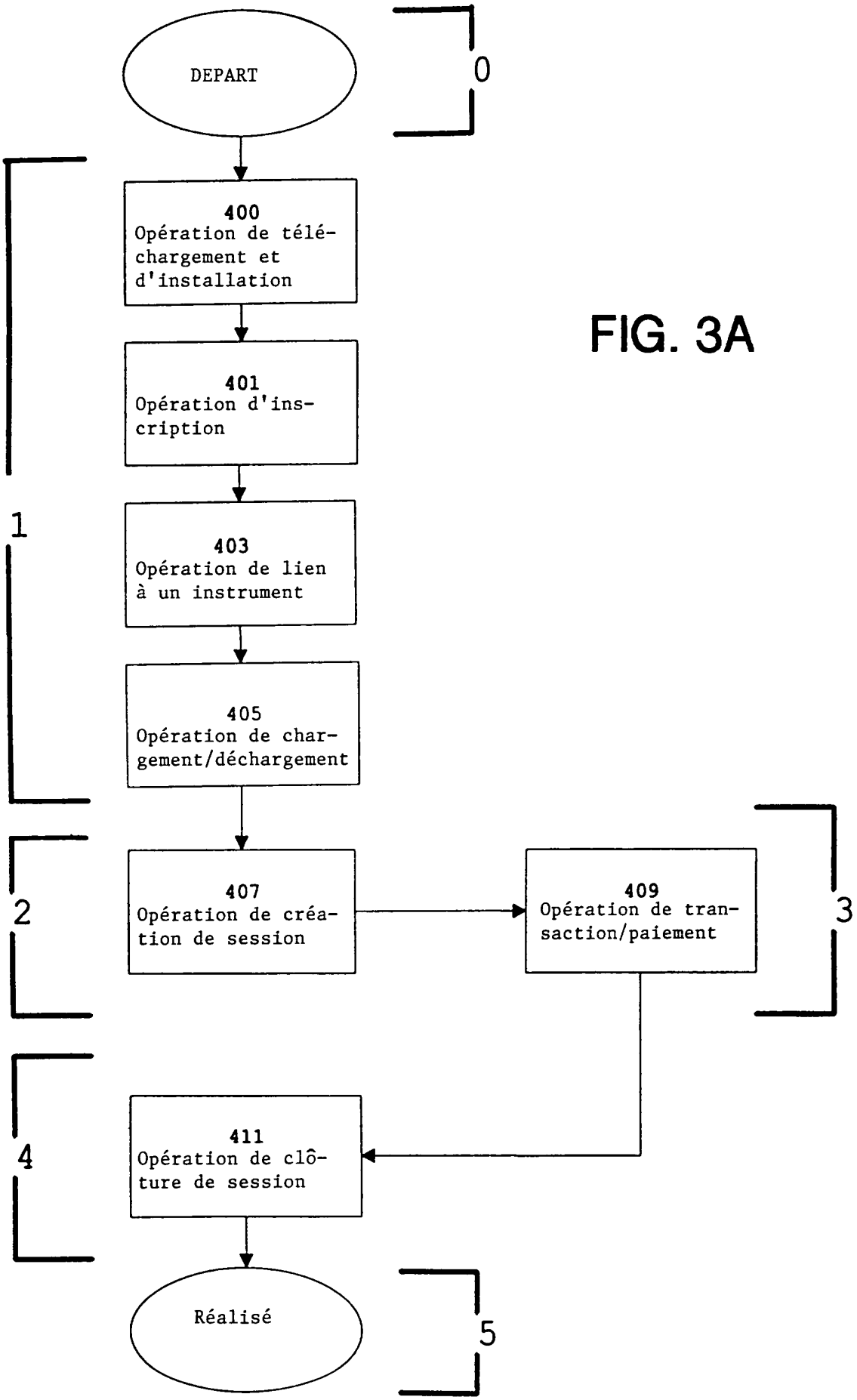

DEPART
0
400
Opération de télé-chargement et d'installation
401
Opération d'ins-cription
403
Opération de lien à un instrument
405
Opération de char-gement/déchargement
1
407
Opération de créa-tion de session
2
409
Opération de tran-saction/paiement
3
411
Opération de clô-ture de session
4
Réalisé
5

FIG. 3A

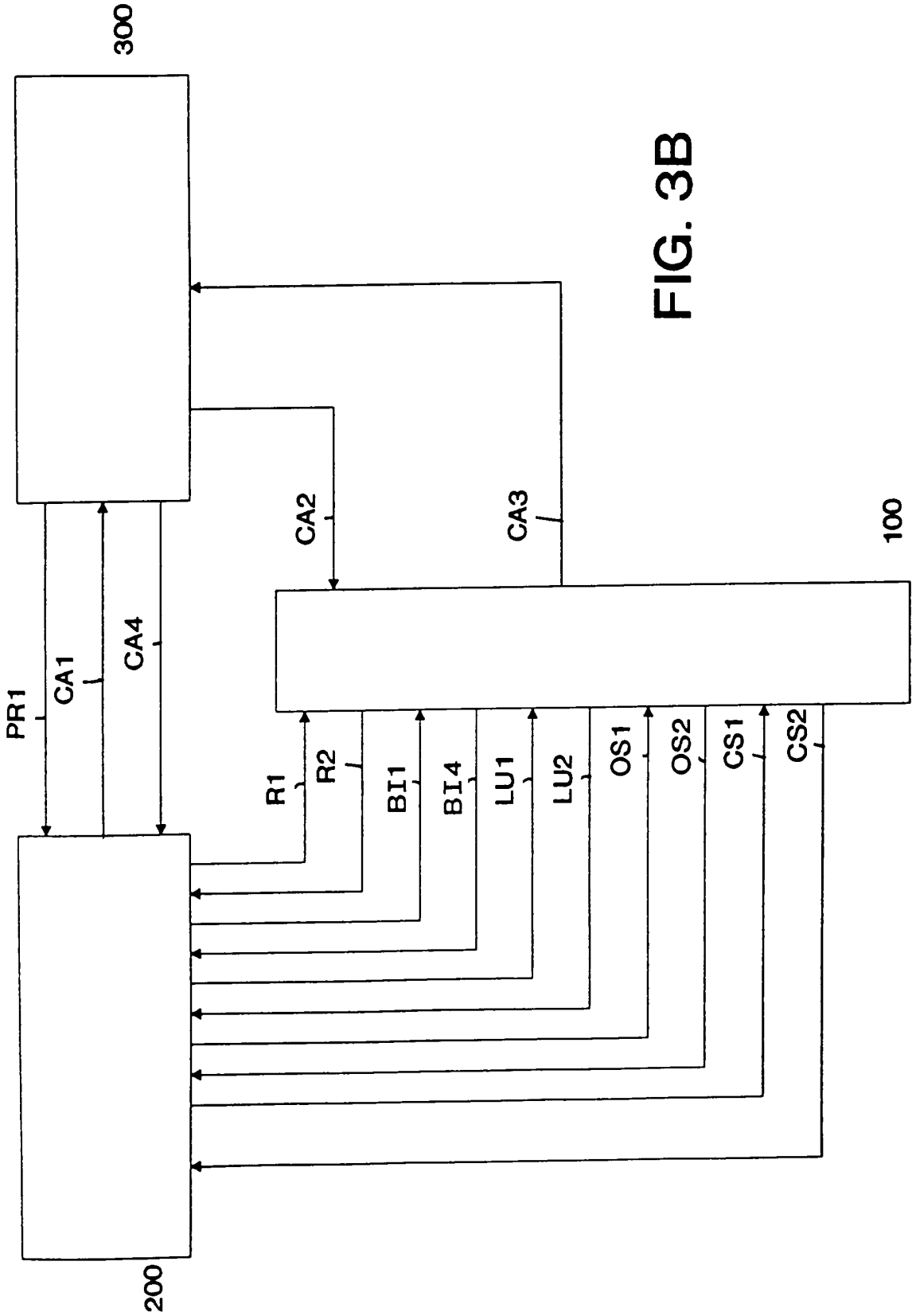

300
100
200
CA1
CA2
CA3
CA4
PR1
R1
R2
BI1
BI4
LU1
LU2
OS1
OS2
CS1
CS2

FIG. 3B

FIG. 4A

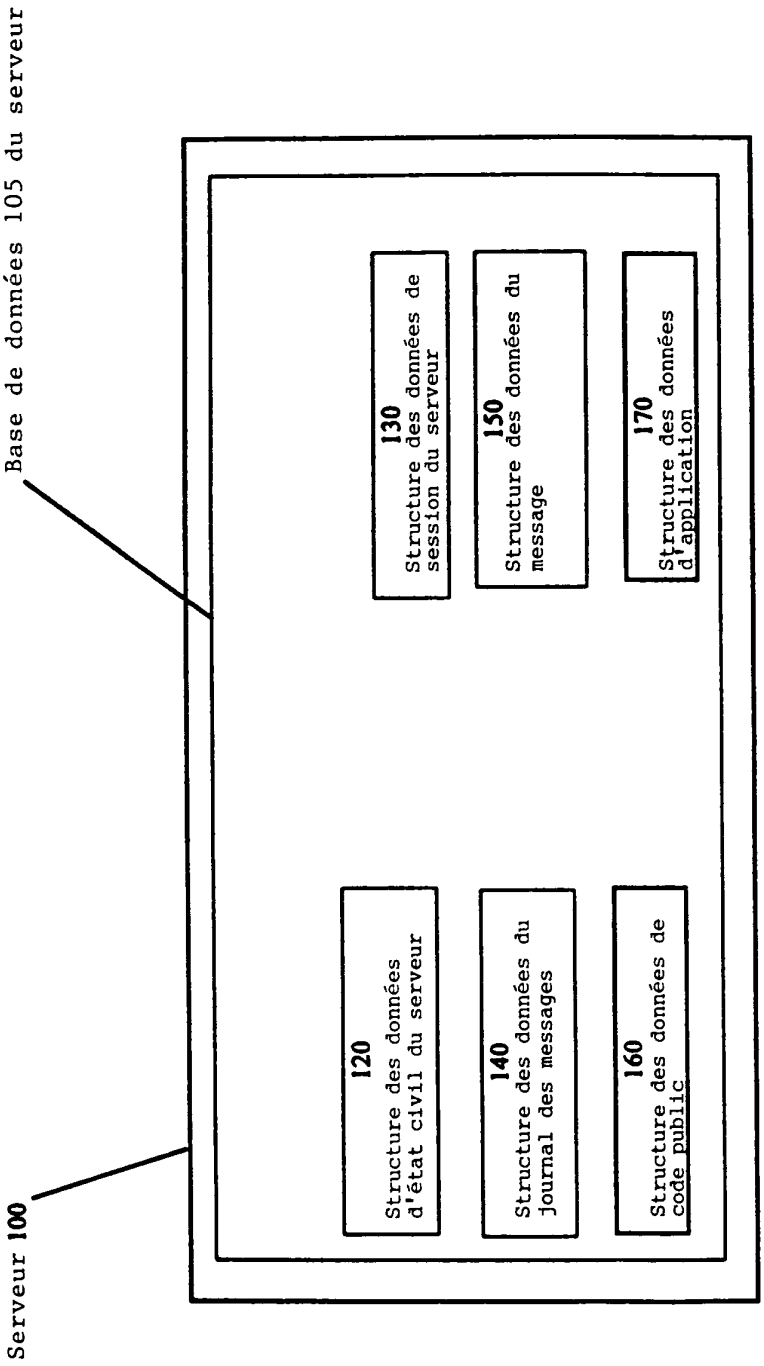

Serveur 100
Base de données 105 du serveur
120
Structure des données d'état civil du serveur
130
Structure des données de session du serveur
140
Structure des données du journal des messages
150
Structure des données du message
160
Structure des données de code public
170
Structure des données d'application

Figure 4B

Tableau illustrant la structure 120 des données d'état civil du serveur

120.1

120A	Etat civil - N° d'identification
120B	Protocole de transport de courrier
120C	Code - Public
120D	Date - Enregistrée
120	Contenu - Langage
120F	Autofermeture - Phrase de passe
120G	Espèces - Conteneur
120H	Instrument - Lien - Date
120I	Accords

Figure 4C

Tableau illustrant les champs des données 120 du conteneur d'espèces

120G.1	Devise
120G.2	Disponible - Balance
120G.3	En suspens - Balance
120G.4	Agence - N° de compte

Figure 4D

Tableau illustrant les champs des données 120H
de lien à un instrument financier

120H.1	Etat civil - N° d'identification
120H.2	Instrument - Type
120H.3	Instrument - Sous-type
120H.4	Instrument - Numéro
120H.5	Instrument - Sous-Numéro
120H.6	Instrument - Devise indigène
120H.7	Accords légaux
120H.8	Instrument - Préfixe
120H.9	Instrument - Contrôle de total de somme
120H.10	Emetteur - N° d'identification
120H.11	Instrument - Nom du détenteur
120H.12	Instrument - Adresse du détenteur
120H.13	Instrument - Lien - Date
120H.14	Instrument - Date 1ère utilisation
120H.15	Etat du lien
120H.16	Transaction de vente - Validée
120H.17	Transaction de vente - Limite
120H.18	Transaction de crédit - Validée
120H.19	Transaction de crédit - Limite
120H.20	Chargement espèces - Validé
120H.21	Chargement espèces - Limite de transaction
120H.22	Déchargement espèces - Validé
120H.23	Déchargement espèces - Limite de transaction
120H.24	Autofermeture - Lien
120H.25	Transaction de vente - Durée limite
120H.26	Transaction de crédit - Durée limite
120H.27	Transaction de chargement - Durée limite
120H.28	Transaction de déchargement - Durée limite

Figure 4E

Tableau illustrant la structure 120 des données d'état civil du serveur

120.2

120AA	Etat civil - N° d'identification
120BB	Protocole de transport de courrier
120CC	Code - Public
120DD	Date - Enregistrée
120	Contenu - Langage
120FF	Autofermeture - Phrase de passe
120GG	Espèces - Conteneur
120HH	Instrument - Lien - Date
120II	Accords

Figure 4F

Tableau illustrant les champs des données 120GG du conteneur d'espèces

120GG.1	Devise
120GG.2	Disponible - Balance
120GG.3	En suspens - Balance
120GG.4	Agence - N° de compte

Figure 4G

Tableau illustrant les champs des données 120HH
de lien à un instrument financier

120HH.1	Etat civil - N° d'identification
120HH.2	Instrument - Type
120HH.3	Instrument - Sous-type
120HH.4	Instrument - Numéro
120HH.5	Instrument - Sous-numéro
120HH.6	Instrument - Devise indigène
120HH.7	Accords légaux
120HH.8	Instrument - Préfixe
120HH.9	Instrument - Contrôle de total de somme
120HH.10	Emetteur - N° d'identification
120HH.11	Instrument - Nom du détenteur
120HH.12	Instrument - Adresse du détenteur
120HH.13	Instrument - Lien - Date
120HH.14	Instrument - Date 1ère utilisation
120HH.15	Etat du lien
120HH.16	Transaction de vente - Validée
120HH.17	Transaction de vente - Limite
120HH.18	Transaction de crédit - Validée
120HH.19	Transaction de crédit - Limite
120HH.20	Chargement espèces - Validé
120HH.21	Chargement espèces - Limite de transaction
120HH.22	Déchargement espèces - Validé
120HH.23	Déchargement espèces - Limite de transaction
120HH.24	Autofermeture - Lien
120HH.25	Transaction de vente - Durée limite
120HH.26	Transaction de crédit - Durée limite
120HH.27	Transaction de chargement - Durée limite
120HH.28	Transaction de déchargement - Durée limite

Figure 4H

Tableau illustrant l'enregistrement d'une session de client de la structure 130 des données d'une session de serveur

130.1

130A	Session - N° d'identification
130B	Session - Code
130C	session - Sel
130D	Devise
130	Ouverture - Montant
130F	Montant - Courant
130G	Ouverture - Date
130H	Clôture - Date
130I	Code - Emploi - Limite
130J	Code - Durée de vie
130K	Etat civil - N° d'identification
130L	Etat
130M	Mémo
130N	Transaction - Données

Figure 4I

Tableau illustrant les champs des données de transaction 130N

130N.1	Montant
130N.2	Payeur - Session - N° d'identification
130N.3	Bénéficiaire - Ordre
130N.4	Bénéficiaire - Session
130N.5	Payeur - Indice

Figure 4J

Tableau illustrant l'enregistrement d'une session de la structure 130 des données d'une session de serveur

130.2

130AA	Session - N° d'identification
130BB	Session - Code
130CC	session - Sel
130DD	Devise
130	Ouverture - Montant
130FF	Montant - Courant
130GG	Ouverture - Date
130HH	Clôture - Date
130II	Code - Emploi - Limite
130JJ	Code - Durée de vie
130KK	Etat civil - N° d'identification
130LL	Etat
130MM	Mémo
130NN	Transaction - Données

Figure 4K

Tableau illustrant les champs des données de transaction 130NN

130NN.1	Montant
130NN.2	Payeur - Session - N° d'identification
130NN.3	Bénéficiaire - Ordre - N° d'identification
130NN.4	Bénéficiaire - Session - N° d'identification
130NN.5	Bénéficiaire - Indice - N° d'identification

Figure 4L

Tableau illustrant l'enregistrement 140.1 de la structure 140 des données du journal de messages

140.1

140A	Etat civil - N° d'identification
140B	Session - N° d'identification
140C	Transaction - Numéro
140E	Message - Entrant
140F	Message - Réponse

FIG. 5A

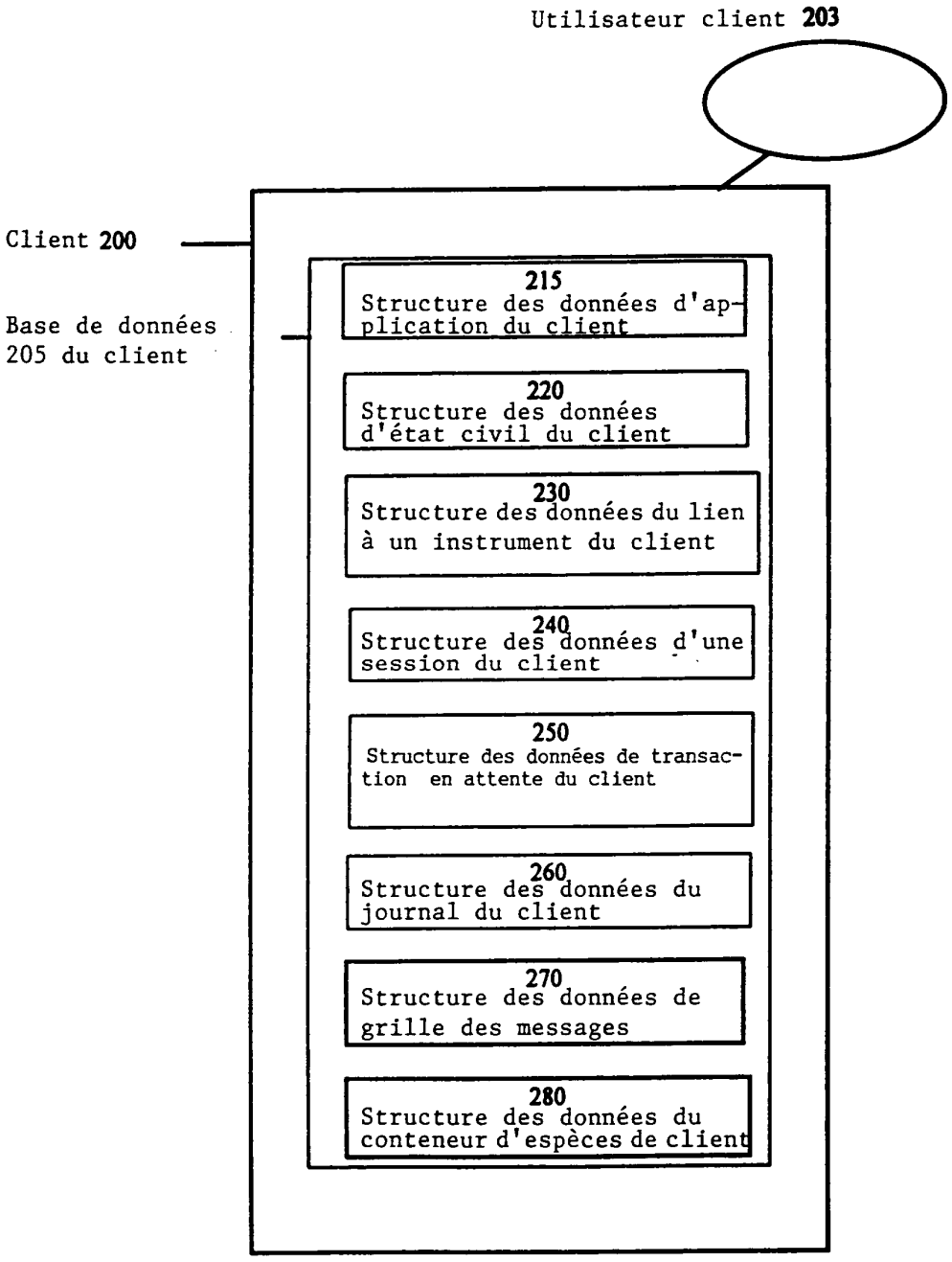

Utilisateur client 203
Client 200
Base de données 205 du client
215 Structure des données d'application du client
220 Structure des données d'état civil du client
230 Structure des données du lien à un instrument du client
240 Structure des données d'une session du client
250 Structure des données de transaction en attente du client
260 Structure des données du journal du client
270 Structure des données de grille des messages
280 Structure des données du conteneur d'espèces de client

Figure 5B

Tableau illustrant l'enregistrement de la structure 215 des données d'application du client

215.1

215A	Serveur - 100 - Code - Public
215B	RRU du serveur - 100

Figure 5C

Tableau illustrant l'enregistrement de la structure 220 des données d'état civil du client

220.1

220A	Client - Etat civil - Numéro d'identification
220B	Protocole de transport de courrier
220C	Code - Public
220D	Autofermeture - Mot de passe
220E	Contenu - Langage
220F	Implicite - Nom et Adresse
220G	Logiciel - Options
220H	Code - Privé
220I	Espèces - Conteneur - Données
220J	Instrument - Date - Lien
220K	Autofermeture - Compte
220L	Accords
220M	Sessions actives - Données
220N	Données - Journal - Attente
220O	Transaction - Données - Journal

Figure 5D

Tableau illustrant l'enregistrement de la structure 230 des données du lien à un instrument financier du client

230.1

230A	Instrument - Numéro
230B	Instrument - Description
230C	Détenteur - Nom
230D	Détenteur - Adresse
230E	Détenteur - Ville
230F	Détenteur - Pays
230G	Détenteur - Code Postal
230H	Détenteur - Code du pays
230I	Détenteur - Code de zone
230J	Détenteur - Téléphone
230K	Devise
230L	Transaction - Vente - Indicateur
230M	Transaction - Crédit - Indicateur
230N	Déchargement - Fonds - Indicateur
230O	Chargement - Fonds - Indicateur
230P	Etat
230Q	Instrument - Sel
230R	Instrument - Donnée - Récurrente
230S	Accords

Figure 5E

Tableau illustrant l'enregistrement de la structure 240 des données d'une session active du client

240.1

240A	Session - N° d'identification
240B	Session - Code
240C	Session - Sel
240D	Devise
240E	Ouverture - Montant
240F	Montant - Courant
240G	Indice
240H	Mémo
240J	Code - Limite - Utilisation
240K	Code - Durée de vie

Figure 5F

Tableau illustrant la structure 250 des données du journal en attente du client

Enregis-trement	Description
251	Information sur l'inscription de l'état civil/ Mise à jour en attente
252	Lien à l'instrument financier en attente, liaison et mise à jour
253	Paiement en espèces en attente
254	Chargement / Déchargement de fonds en attente
255	Ouverture de session en attente
256	Clôture de session en attente

Figure 5G

Tableau illustrant l'enregistrement d'une inscription en attente / enregistrement d'une mise à jour d'information d'état civil

251A	Transaction - Type
251B	Transaction - Numéro
251C	Transaction - Date/Temps
251D	Logiciel - Version
251E	Langage
251F	Devise
251G	N° d'état civil demandé
251H	Protocole de transport de courrier - Adresse
251I	Autofermeture - Phrase de passe
251J	Chaîne - Transaction - Origine

Figure 5H

Tableau illustrant l'enregistrement d'une liaison en attente/ mise à jour du lien à un instrument

252

252A	Transaction - Type
252B	Transaction - Numéro
252C	Transaction - Date/temps
252D	Logiciel - Version
252E	Etat civil - N° d'identification
252F	Instrument - Numéro
252G	Client - N° d'identification
252H	Nom sur carte
252I	Instrument - Date d'expiration
252J	Détenteur - Adresse
252K	Détenteur - Ville
252L	Détenteur - Etat
252M	Détenteur - Code postal
252N	Détenteur - Pays
252O	Détenteur - Code - Pays
252P	Détenteur - Code - Zone
252Q	Détenteur - Téléphone
252R	Description de carte
252S	Instrument - Donnée récurrente
252T	Instrument - Type
252U	Sel
252V	Autofermeture - Indicateur - Compte
252W	Transaction - Originale - Chaîne

Figure 5I

Tableau illustrant l'enregistrement d'un paiement en espèces en attente

253

253A	Transaction - Type
253B	Transaction - Numéro
253C	Transaction - Date/temps
253D	Logiciel - Version
253	Etat civil - N° d'identification
253F	Ordre - N° d'identification
253G	Commerçant - N° d'identification
253H	Montant
253J	Payés à RRU
253K	Session - N° d'identification
253L	Indice
253M	Chaîne - Transaction - Originale
253N	RRU - Annulation
253O	RRU - Succès
253P	RRU - Echec

Figure 5J

Tableau illustrant l'enregistrement d'un chargement/déchargement de fonds en attente

254

254A	Transaction - Type
254B	Transaction - Numéro
254C	Transaction - Date/Temps
254D	Logiciel - Version
254E	Etat-Civil - Numéro d'identification
254F	Instrument - Numéro de compte
254G	Montant
254H	Type de compte
254I	Chaîne de transaction d'origine

Figure 5K

Tableau illustrant un enregistrement d'ouverture de session en attente

255

255A	Transaction - Type
255B	Transaction - Numéro
255C	Transaction - Date/Temps
255D	Logiciel - Version
255E	Etat Civil - Numéro d'identification
255F	Montant
255G	Code - Limite d'utilisation demandée
255H	Code - Durée de vie demandée
255I	Session - Utilisateur - Description
255J	Devise
255K	Chaîne de transaction d'origine

Figure 5L

Tableau illustrant un enregistrement de clôture de session en attente

256

256A	Transaction - Type
256B	Transaction - Numéro
256C	Transaction - Date/Temps
256D	Logiciel - Version
256E	Etat Civil - Numéro d'identification
256F	Transaction - Journal
256G	Session - Numéro d'identification
256H	Session - Utilisateur - Description
256I	Chaîne de transaction d'origine

Figure 5M

Tableau illustrant la structure 260 des données du journal du client

Record	Description
261	Réponse à une information d'inscription/ Mise à jour d'état civil
262	Réponse à la liaison/Mise à jour du lien à un instrument
263	Réponse au paiement en espèces
264	Réponse au chargement/déchargement de fonds
265	Réponse à une ouverture de session
266	Demande de paiement
267	Réponse à une clôture de session

Figure 5N

Tableau illustrant l'enregistrement d'une réponse à l'inscription/mise à jour d'un état civil

261

261A	Transaction - Type
261B	Transaction - Numéro
261C	Transaction - Date/Temps
261D	Logiciel - Code de sévérité
261E	Logiciel - Message
261F	Réponse - Code
261G	Réponse - Message
261H	Numéro d'identification d'état civil demandé
261I	Numéro d'identification d'état civil suggéré
261J	Protocole de transport de courrier - Adresse
261K	Langage
261L	Devise

Figure 50

Tableau illustrant l'enregistrement d'une réponse à une liaison/mise à jour d'un instrument

262

262A	Transaction - Type
262B	Transaction - Numéro
262C	Transaction - Date/Temps
262D	Logiciel - Code de sévérité
262E	Logiciel - Message
262F	Réponse - Code
262G	Réponse - Message
262H	Etat civil - Numéro d'identification
262I	Instrument - Numéro
262J	Instrument - Type
262K	Client - Numéro d'identification
262L	Nom sur carte
262M	Instrument - Date d'expiration
262N	Détenteur - Adresse
262O	Détenteur - Ville
262P	Détenteur - Etat
262Q	Détenteur - Code postal
262R	Détenteur - Pays
262S	Détenteur - Code de pays
262T	Détenteur - Code de zone
262U	Détenteur - Téléphone
262V	Description de l'instrument
262W	Devise
262X	Emetteur
262Y	Emetteur - Pays
262Z	Autofermeture - Indicateur

Figure 5P

Tableau illustrant l'enregistrement de réponse à un paiement en espèces

263

263A	Transaction - Type
263B	Transaction - Numéro
263C	Transaction - Date/Temps
263D	Réponse - Code
263E	Réponse - Message
263F	Etat civil - Numéro d'identification
263G	Ordre - Numéro d'identification
263H	Commerçant - Numéro d'identification
263I	Commerçant - Message
263J	Montant
263K	Utilisateur - Mémo
263L	Session - Numéro d'identification
263M	Indice

Figure 5Q

Tableau illustrant la réponse à un chargement/déchargement

264A	Transaction - Type
264B	Transaction - Numéro
264C	Transaction - Date/Temps
264D	Logiciel - Code de sévérité
264E	Logiciel - Message
264F	Réponse - Code
264G	Réponse - Message
264H	Etat civil - Numéro d'identification
264I	Instrument - Numéro de compte
264J	Montant
264K	Honoraire
264L	Balance
264M	Balance en suspens

Figure 5R

Tableau illustrant l'enregistrement de la réponse à une ouverture de session

265

265A	Transaction - Type
265B	Transaction - Numéro
265C	Transaction - Date/Temps
265D	Logiciel - Code de sévérité
265E	Logiciel - Message
265F	Réponse - Code
265G	Réponse - Message
265H	Etat civil - Numéro d'identification
265I	Montant
265J	Code - Limite d'utilisation accordée
265K	Code - Durée de vie
265L	Session - Numéri d'identification
265M	Session - Utilisateur - Description
265N	Honoraire
265O	Balance

Figure 5S

Tableau illustrant l'enregistrement d'une demande de paiement

266

266A	Commerçant - Numéro d'identification
266B	Ordre - Numéro d'identification
266C	Montant(s)
266D	Crédit - Cartes - Accepté
266E	Commerçant - Note
266F	Payer à RRU

Figure 5T

Tableau illustrant l'enregistrement d'une réponse à une clôture de session

267

267A	Transaction - Type
267B	Transaction - Numéro
267C	Transaction - Date/Temps
267D	Logiciel - Code de sévérité
267E	Logiciel - Message
267F	Réponse - Code
267G	Réponse - Message
267H	Etat civil - Numéro d'identification
267I	Montant
267J	Transaction - Journal
267K	Honoraire

Figure 5U

Tableau illustrant l'enregistrement de la structure 280 des données du conteneur d'espèces du client

280.1

280A	Devise
280B	Disponible - Balance
280C	En suspens - Balance

FIG. 6A

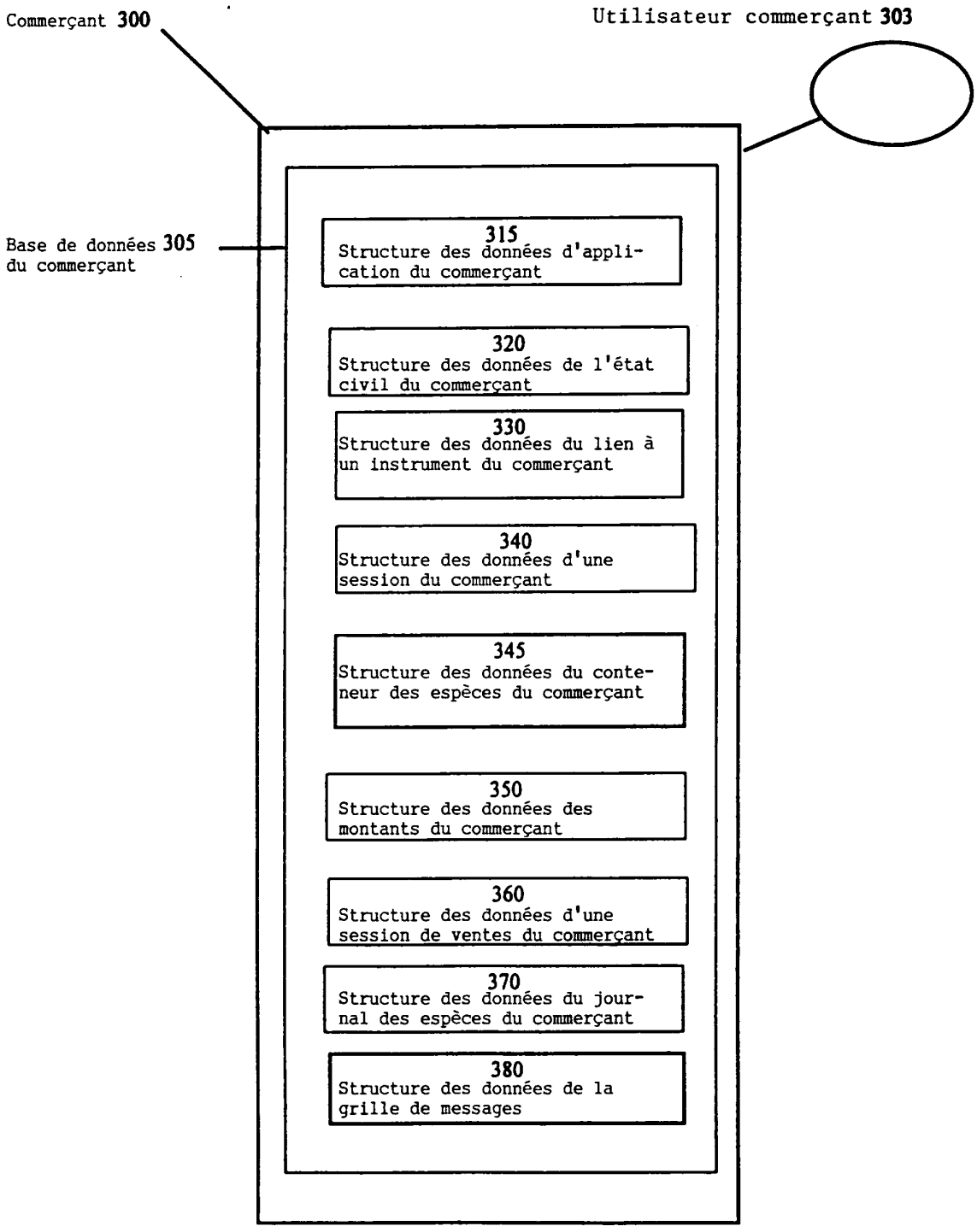

Commerçant 300
Utilisateur commerçant 303
Base de données 305 du commerçant
315 Structure des données d'application du commerçant
320 Structure des données de l'état civil du commerçant
330 Structure des données du lien à un instrument du commerçant
340 Structure des données d'une session du commerçant
345 Structure des données du conteneur des espèces du commerçant
350 Structure des données des montants du commerçant
360 Structure des données d'une session de ventes du commerçant
370 Structure des données du journal des espèces du commerçant
380 Structure des données de la grille de messages

Figure 6B

Tableau illustrant l'enregistrement de la structure 315 des données d'application du commerçant

315A	Serveur - 100 - Code public
315B	RRU du serveur 100

Figure 6C

Tableau illustrant la structure 320 des données d'état civil du client

320A	Commerçant - Etat civil - Numéro d'identification
320B	Protocole de transport de courrier
320C	Code public
320D	Date enregistrée
320E	Contenu - Langage
320F	Nom et adresse implicites
320G	Logiciel - Options
320H	Code privé
320I	Instrument - Données du lien
320J	Espèces - Conteneur - Données

Figure 6D

Tableau illustrant l'enregistrement de la structure 330 des données du lien à un instrument du commerçant

330A	Instrument - Numéro
330B	Instrument - Description
330C	Détenteur - Nom
330D	Détenteur - Adresse
330E	Détenteur - Ville
330F	Détenteur - Pays
330G	Détenteur - Code postal
330H	Détenteur - Code du pays
330I	Détenteur - Code de zone
330J	Détenteur - Téléphone
330K	Devise
330L	Transaction - Vente - Indicateur
330M	Transaction - Crédit - Indicateur
330N	Déchargement - Fonds - Indicateur
330O	Chargement - Fonds - Indicateur
330P	Etat
330Q	Instrument - Sel
330R	Instrument - Donnée récurrente
330S	Accords

Figure 6E

Tableau illustrant l'enregistrement de la structure 340 des données d'une session du commerçant

340A	Session - Numéro d'identification
340B	Session - Code
340C	Session - Sel
340D	Devise
340E	Montant à l'ouverture
340F	Montant courant
340G	Date d'ouverture
340H	Date de clôture
340J	Code - Limite d'utilisation
340K	Code - Durée de vie

Figure 6F

Tableau illustrant l'enregistrement de la structure 390 des données du conteneur d'espèces du commerçant

390A	Devise
390B	Disponible - Balance
390C	En suspens - Balance

FIGURE 7

Figure 7A

Tableau illustrant l'enregistrement de la structure 350 des données des montants du commerçant

350A	Ordre - Numéro d'identification
350B	Montant de la transaction
350C	Indicateur

Figure 7B

Tableau illustrant l'enregistrement de la structure 360 des données d'une session de ventes du commerçant

360A	Session - Numéro d'identification
360B	Session - Code
360C	Session - Sel
360D	Devise
360E	Mémo
360F	Montant courant
360G	Date d'ouverture
360H	Date de clôture
360I	Etat
360J	Code - Limite d'utilisation
360K	Code - Durée de vie
360L	Etat civil - Numéro d'identification

Figure 7C

Tableau illustrant l'enregistrement de la structure 370 des données du journal des espèces du commerçant

370A	Type
370B	Etat
370C	Ordre - Numéro d'identification
370D	Client - Numéro d'identification - Session
370E	Client - Indice - Numéro
370F	Client - Devise
370G	Commerçant - Numéro d'identification - Session
370H	Commerçant - Numéro d'indice
370I	Commerçant - Devise
370J	Commerçant - Montant demandé
370K	Montant - Crédité
370L	Honoraires - Payés
370M	Résultat - Code
370N	Type
370O	Etat
370P	Transaction - Numéro
370Q	Durée de session demandée
370R	Compte de session demandé
370S	Session - Numéro d'identification
370T	Résultat - Code

Figure 7D

Tableau illustrant le format du message échantillon 4000

4000

4010

4005	[En-Tête]
4013A	Libellé 1 : Valeur 1
4013B	Libellé 2 : Valeur 2
4017	Opaque :
4050	[Queue]

FIGURE 8

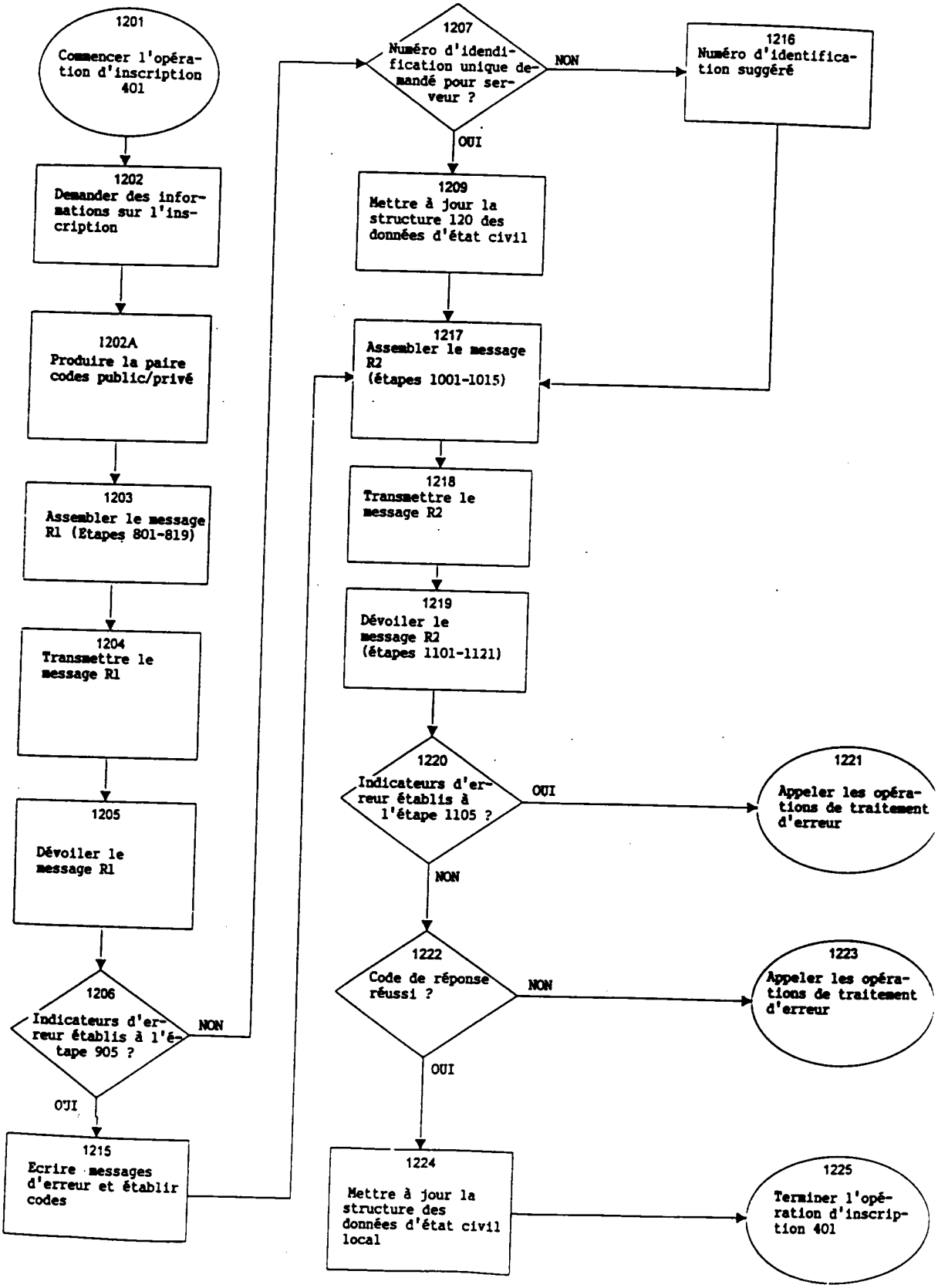

1201
Commencer l'opération d'inscription 401
1202
Demander des informations sur l'inscription
1202A
Produire la paire codes public/privé
1203
Assembler le message R1 (Etapes 801-819)
1204
Transmettre le message R1
1205
Dévoiler le message R1
1206
Indicateurs d'erreur établis à l'étape 905 ?
NON
OUI
1215
Ecrire messages d'erreur et établir codes
1207
Numéro d'identification unique demandé pour serveur ?
NON
OUI
1216
Numéro d'identification suggéré
1209
Mettre à jour la structure 120 des données d'état civil
1217
Assembler le message R2 (étapes 1001-1015)
1218
Transmettre le message R2
1219
Dévoiler le message R2 (étapes 1101-1121)
1220
Indicateurs d'erreur établis à l'étape 1105 ?
OUI
NON
1221
Appeler les opérations de traitement d'erreur
1222
Code de réponse réussi ?
NON
OUI
1223
Appeler les opérations de traitement d'erreur
1224
Mettre à jour la structure des données d'état civil local
1225
Terminer l'opération d'inscription 401

FIGURE 9

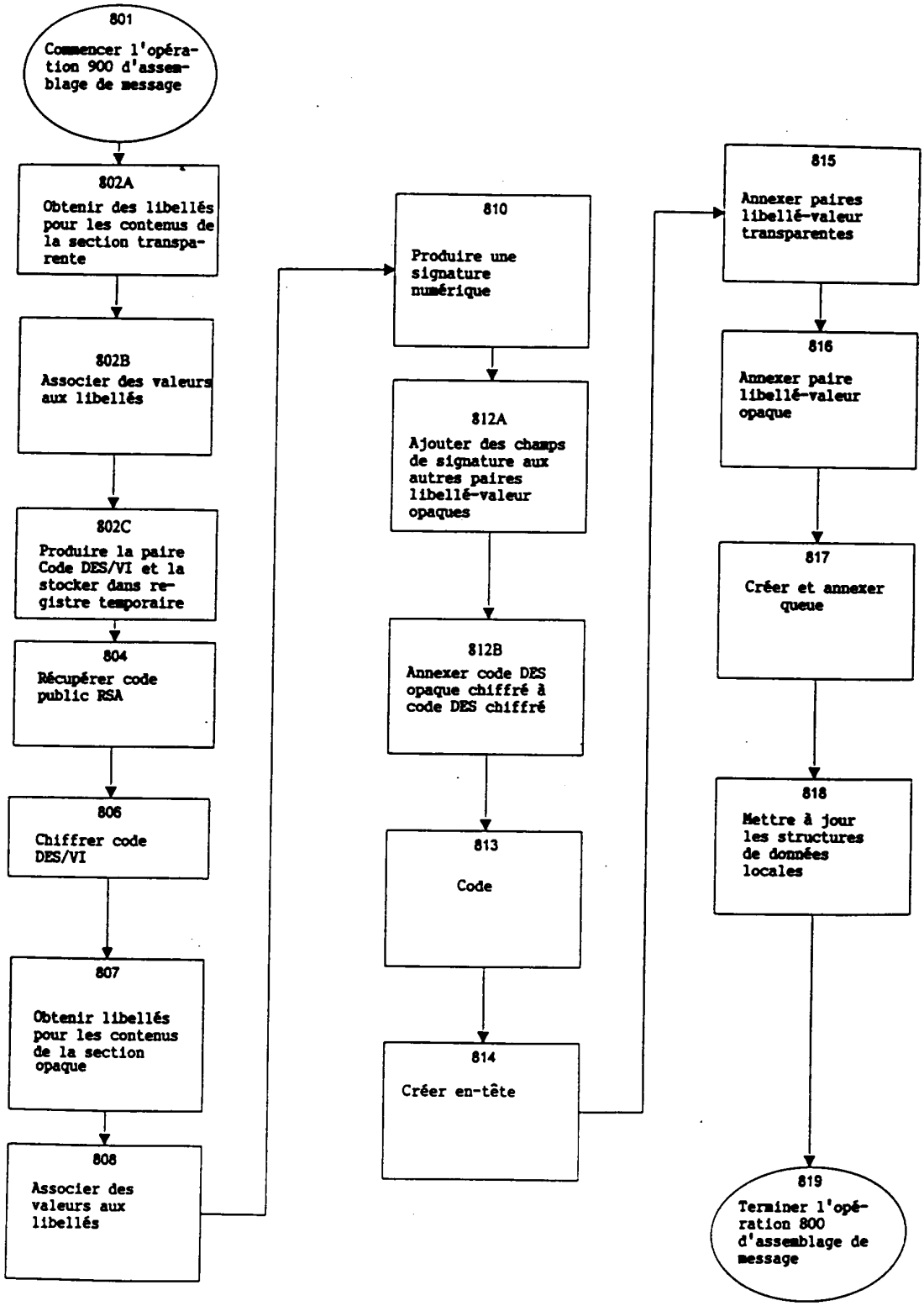

801
Commencer l'opération 900 d'assemblage de message
802A
Obtenir des libellés pour les contenus de la section transparente
802B
Associer des valeurs aux libellés
802C
Produire la paire Code DES/VI et la stocker dans registre temporaire
804
Récupérer code public RSA
806
Chiffrer code DES/VI
807
Obtenir libellés pour les contenus de la section opaque
808
Associer des valeurs aux libellés
810
Produire une signature numérique
812A
Ajouter des champs de signature aux autres paires libellé-valeur opaques
812B
Annexer code DES opaque chiffré à code DES chiffré
813
Code
814
Créer en-tête
815
Annexer paires libellé-valeur transparentes
816
Annexer paire libellé-valeur opaque
817
Créer et annexer queue
818
Mettre à jour les structures de données locales
819
Terminer l'opération 800 d'assemblage de message

FIGURE 10A

Tableau illustrant le format du message R1

4205	[En-tête]
4213A	Transaction :
4213B	Date :
4213C	Code du serveur :
4213D	Service - Catégorie :
4217	Opaque :
4250	[Queue]

FIGURE 10B

Tableau illustrant les contenus de la section opaque du message R1

4217A	Type :
4217B	Serveur - Date :
4217C	Version de logiciel :
4217D	Contenu - Langage :
4217E	Devise implicite :
4217F	Numéro d'identification demandé :
4217G	Protocole de transport de courrier :
4217H	Accords :
4217I	Autofermeture - Phrase de passe :
4217J	Code public :
4217K	Signature :

FIGURE 11A

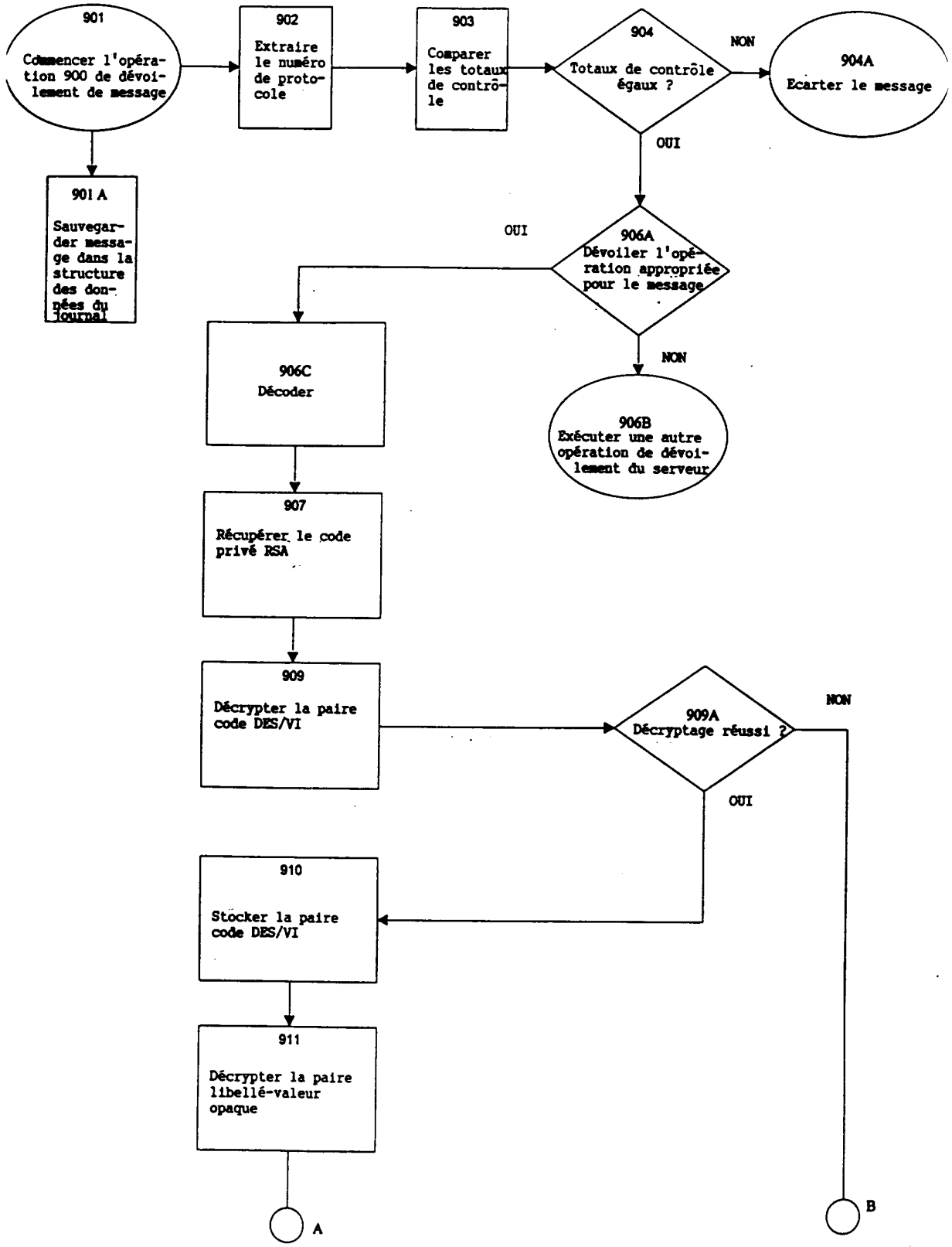

901
Commencer l'opération 900 de dévoilement de message
902
Extraire le numéro de protocole
903
Comparer les totaux de contrôle
904
Totaux de contrôle égaux ?
NON
904A
Ecarter le message
OUI
901A
Sauvegarder message dans la structure des données du journal
OUI
906A
Dévoiler l'opération appropriée pour le message
NON
906C
Décoder
906B
Exécuter une autre opération de dévoilement du serveur
907
Récupérer le code privé RSA
909
Décrypter la paire code DES/VI
909A
Décryptage réussi ?
NON
OUI
910
Stocker la paire code DES/VI
911
Décrypter la paire libellé-valeur opaque
A
B

FIGURE 11B

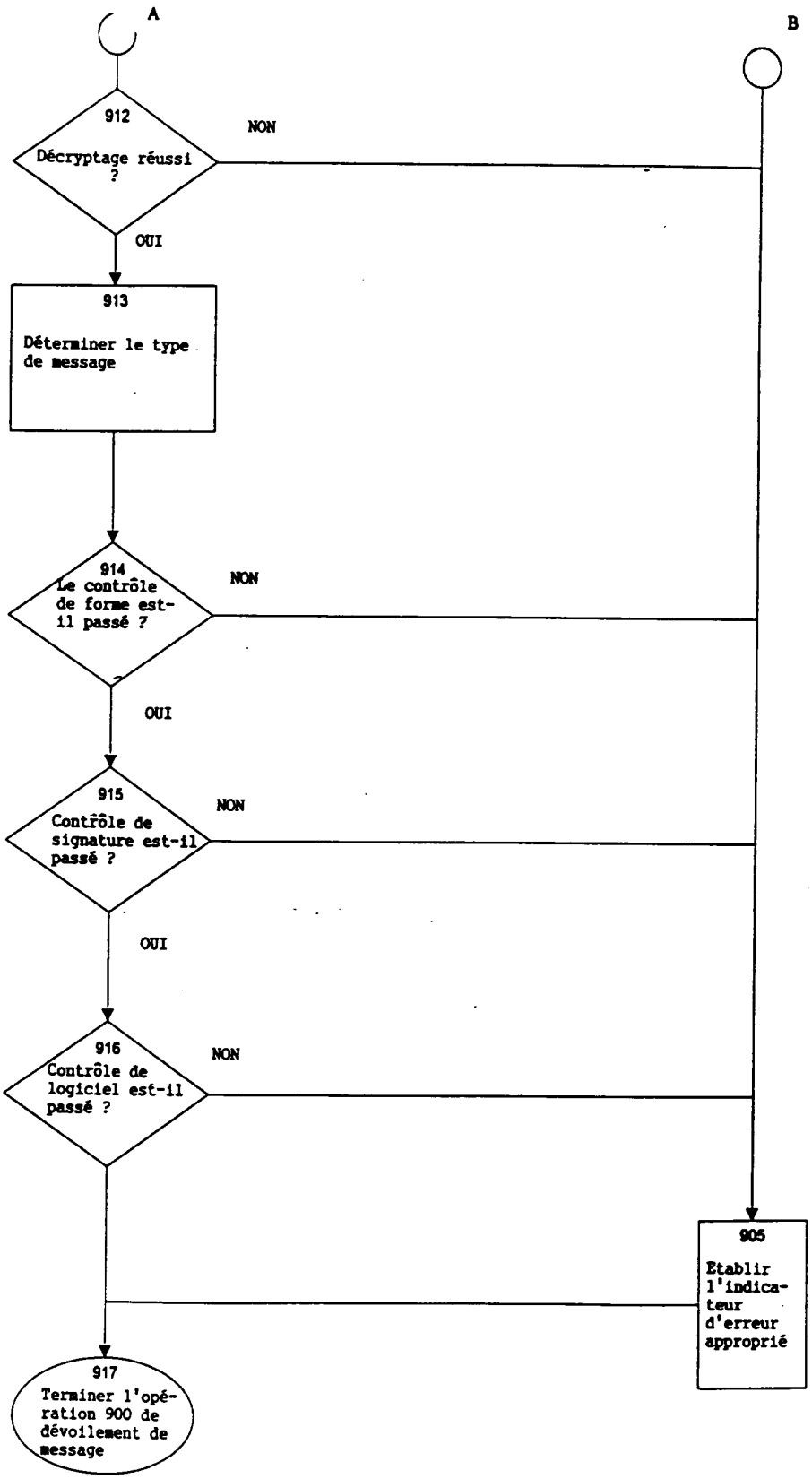

A
B
912
Décryptage réussi ?
NON
OUI
913
Déterminer le type de message
914
Le contrôle de forme est-il passé ?
NON
OUI
915
Contrôle de signature est-il passé ?
NON
OUI
916
Contrôle de logiciel est-il passé ?
NON
905
Etablir l'indicateur d'erreur approprié
917
Terminer l'opération 900 de dévoilement de message

FIGURE 12

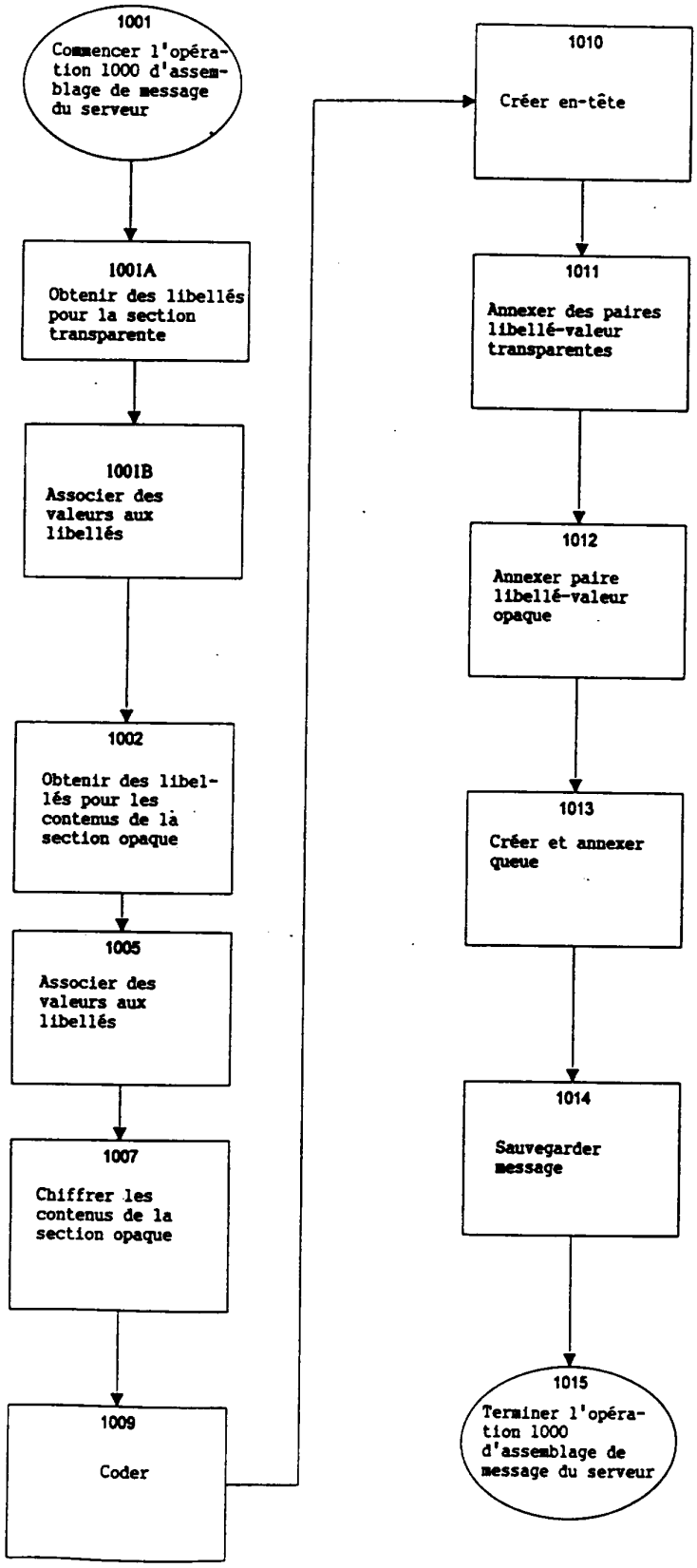

1001
Commencer l'opération 1000 d'assemblage de message du serveur
1001A
Obtenir des libellés pour la section transparente
1001B
Associer des valeurs aux libellés
1002
Obtenir des libellés pour les contenus de la section opaque
1005
Associer des valeurs aux libellés
1007
Chiffrer les contenus de la section opaque
1009
Coder
1010
Créer en-tête
1011
Annexer des paires libellé-valeur transparentes
1012
Annexer paire libellé-valeur opaque
1013
Créer et annexer queue
1014
Sauvegarder message
1015
Terminer l'opération 1000 d'assemblage de message du serveur

FIGURE 13A

Tableau illustrant le format du message R2

4305	[En-tête]
4313A	Transaction :
4313B	Date :
4313C	Service - Catégorie :
4317	Opaque :
4350	[Queue]

FIGURE 13B

Tableau illustrant les contenus de la section opaque du message R2

4317A	Type :
4317B	Serveur - Date :
4317C	Numéro d'identification demandé :
4317D	Numéro d'identification de la réponse :
4317E	protocole de transport du courrier :
4317F	Réponse - Code :
4317G	Autofermeture - Phrase de passe :
4317H	Code public :
4317I	Sévérité du logiciel :
4317J	Message du logiciel :
4317K	Message :

FIGURE 14

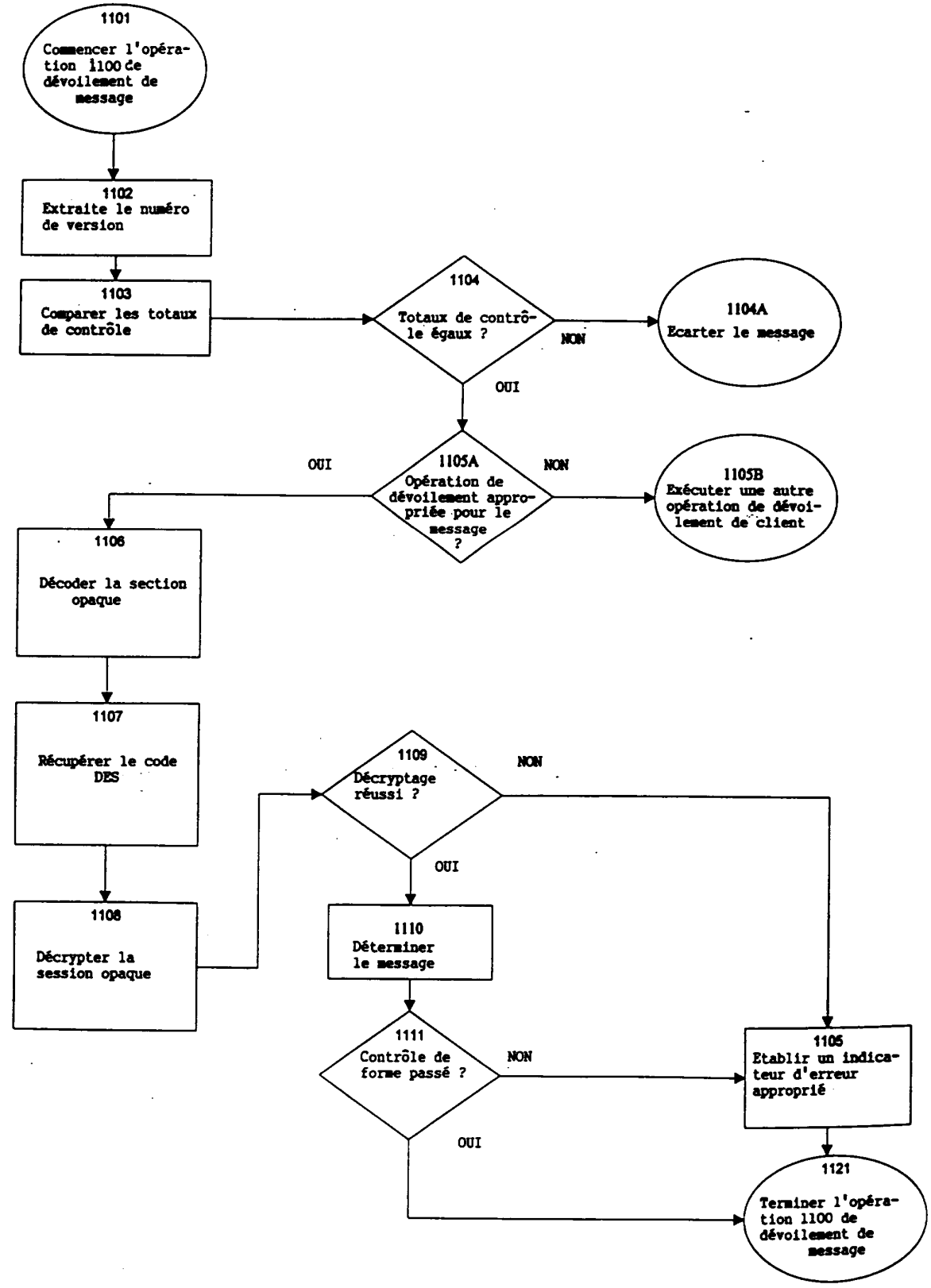

1101
Commencer l'opération 1100 de dévoilement de message
1102
Extraite le numéro de version
1103
Comparer les totaux de contrôle
1104
Totaux de contrôle égaux ?
NON
1104A
Ecarter le message
OUI
1105A
Opération de dévoilement appropriée pour le message ?
OUI
NON
1105B
Exécuter une autre opération de dévoilement de client
1106
Décoder la section opaque
1107
Récupérer le code DES
1108
Décrypter la session opaque
1109
Décryptage réussi ?
NON
OUI
1110
Déterminer le message
1111
Contrôle de forme passé ?
NON
OUI
1105
Etablir un indicateur d'erreur approprié
1121
Terminer l'opération 1100 de dévoilement de message

FIGURE 15

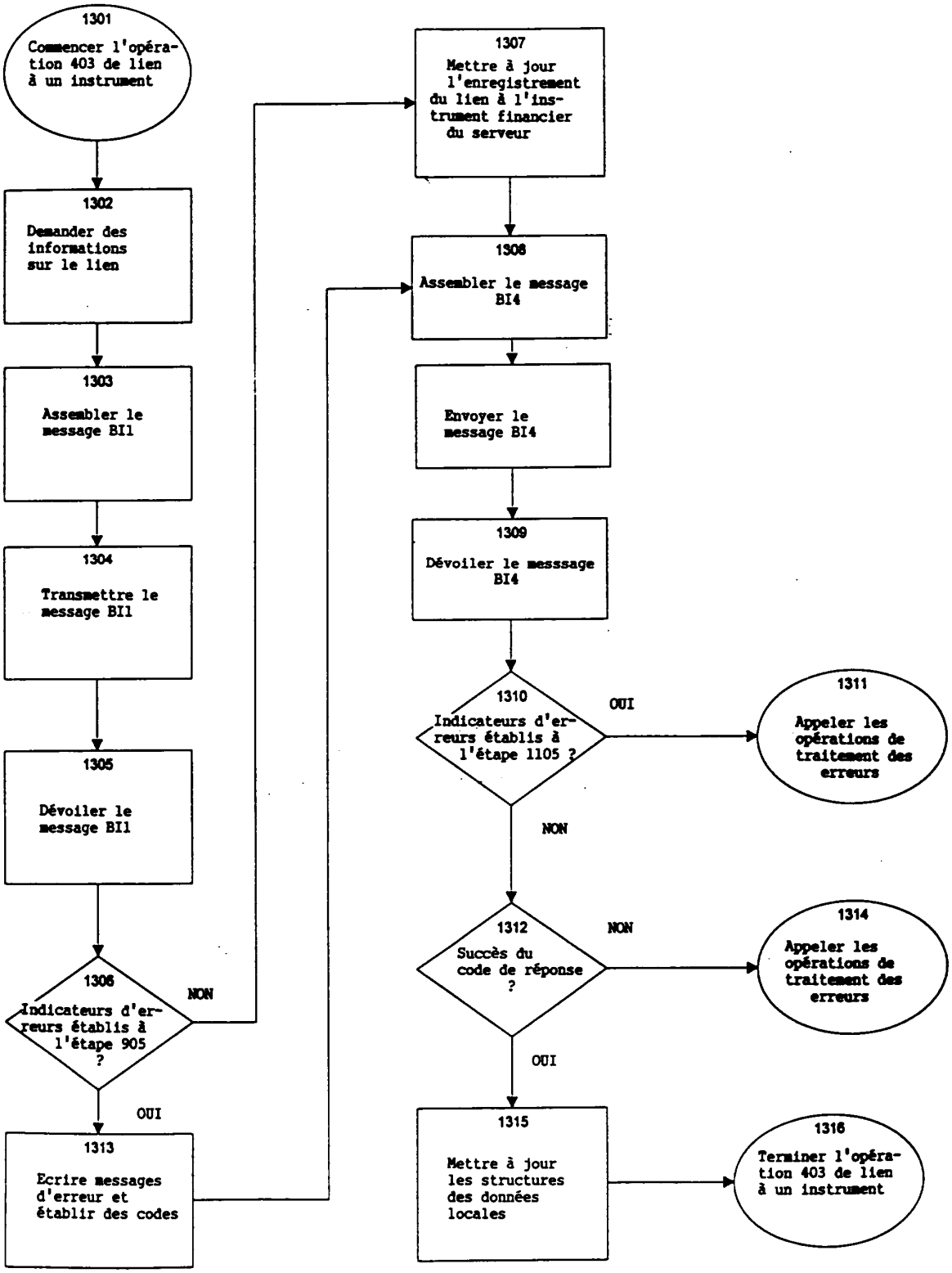

1301
Commencer l'opération 403 de lien à un instrument
1302
Demander des informations sur le lien
1303
Assembler le message BI1
1304
Transmettre le message BI1
1305
Dévoiler le message BI1
1306
Indicateurs d'erreurs établis à l'étape 905 ?
NON
OUI
1313
Ecrire messages d'erreur et établir des codes
1307
Mettre à jour l'enregistrement du lien à l'instrument financier du serveur
1308
Assembler le message BI4
Envoyer le message BI4
1309
Dévoiler le messsage BI4
1310
Indicateurs d'erreurs établis à l'étape 1105 ?
OUI
1311
Appeler les opérations de traitement des erreurs
NON
1312
Succès du code de réponse ?
NON
1314
Appeler les opérations de traitement des erreurs
OUI
1315
Mettre à jour les structures des données locales
1316
Terminer l'opération 403 de lien à un instrument

FIGURE 16A

Tableau illustrant le format du message BI1

4405	[En-tête]
4413A	Numéro d'identification d'état civil :
4413B	Transaction :
4413C	Date :
4413D	Code su serveur :
4413E	Service - Catégorie :
4417	Opaque :
4450	[Queue]

FIGURE 16B

Tableau illustrant les contenus de la section opaque du message BI1

4417A	Type :
4417B	Serveur - Date :
4417C	Version du logiciel :
4417D	Instrument - Numéro :
4417E	Instrument - Type :
4417F	Instrument - Catégorie :
4417I	Instrument - Fonctions :
4417J	Instrument - Sel :
4417K	Instrument - Date d'expiration :
4417L	Instrument - Nom :
4417M	Instrument - Rue :
4417N	Instrument - Ville :
4417O	Instrument - Etat
4417P	Instrument - Code postal :
4417Q	Instrument - Pays :
4417R	Accords
4417S	Autofermeture :
4417T	Autofermeture - Phrase de passe :
4417U	Code :
4417V	Signature :

FIGURE 17A

Tableau illustrant le format du message BI4

44.105	[En-tête]
44.113A	Numéro d'identification :
44.113B	Transaction :
44.113C	Date :
44.113D	Service - Catégorie :
44.117	Opaque :
44.150	[Queue]

FIGURE 17B

Tableau illustrant les contenus de la section opaque du message BI4

44.117A	Type :
44.117B	Serveur - Date :
44.117C	Réponse - Code
44.117D	Sévérité du logiciel
44.117	Message du logiciel
44.117F	Instrument - Numéro :
44.117G	Instrument - Type :
44.117H	Instrument - Sel :
44.117J	Instrument - Fonctions :
44.117K	Instrument* :
44.117L	Message ;

FIGURE 18

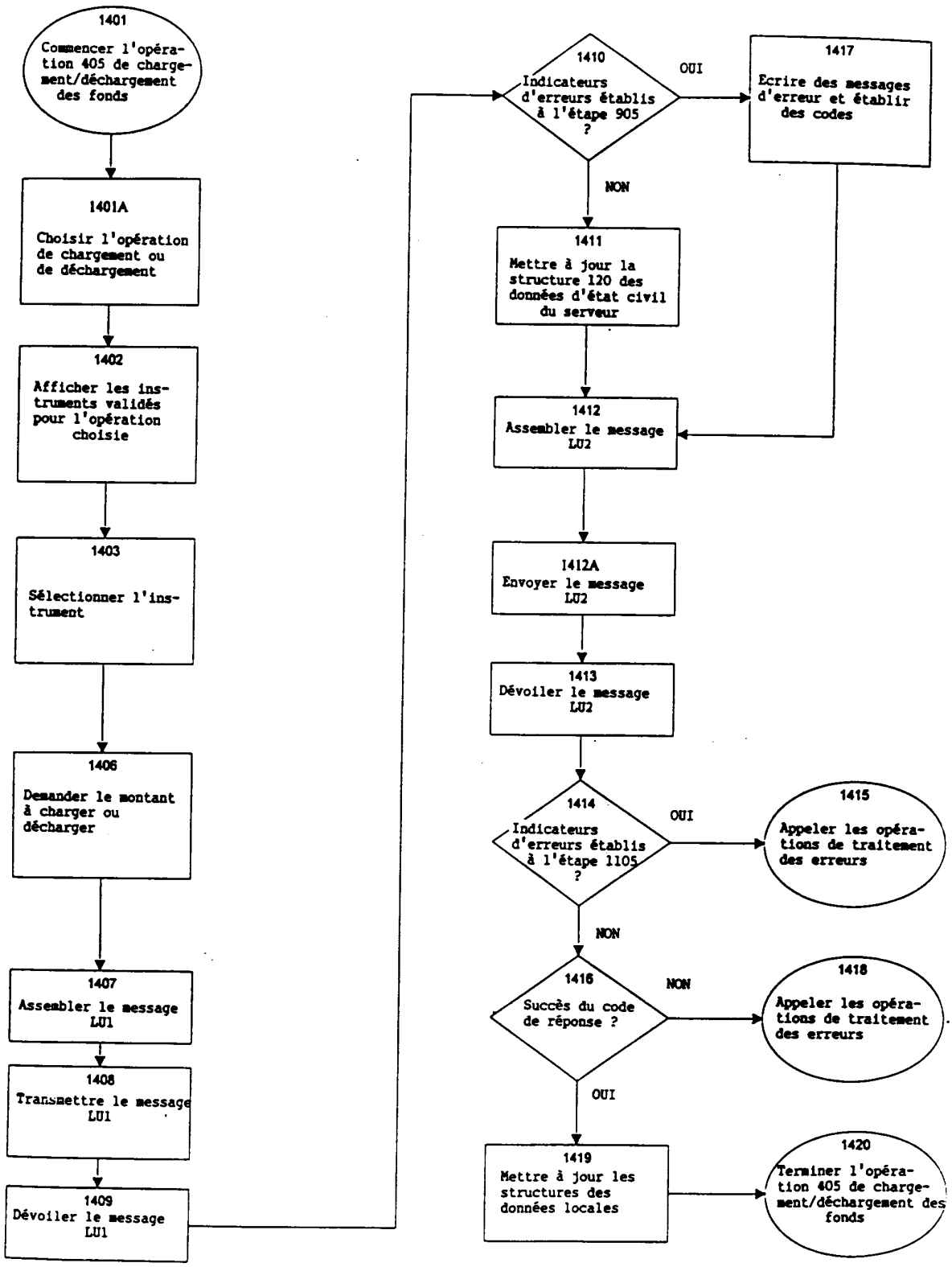

1401
Commencer l'opération 405 de chargement/déchargement des fonds
1401A
Choisir l'opération de chargement ou de déchargement
1402
Afficher les instruments validés pour l'opération choisie
1403
Sélectionner l'instrument
1406
Demander le montant à charger ou décharger
1407
Assembler le message LU1
1408
Transmettre le message LU1
1409
Dévoiler le message LU1
1410
Indicateurs d'erreurs établis à l'étape 905 ?
OUI
NON
1417
Ecrire des messages d'erreur et établir des codes
1411
Mettre à jour la structure 120 des données d'état civil du serveur
1412
Assembler le message LU2
1412A
Envoyer le message LU2
1413
Dévoiler le message LU2
1414
Indicateurs d'erreurs établis à l'étape 1105 ?
OUI
NON
1415
Appeler les opérations de traitement des erreurs
1416
Succès du code de réponse ?
NON
OUI
1418
Appeler les opérations de traitement des erreurs
1419
Mettre à jour les structures des données locales
1420
Terminer l'opération 405 de chargement/déchargement des fonds

FIGURE 19A

Tableau illustrant le format du message LU1

4505	[En-tête]
4513A	Numéro d'identification :
4513B	Transaction :
4513C	Date :
4513D	Code du serveur :
4513e	Service-catégorie :
4517	Opaque :
4550	[Queue]

FIGURE 19B

Tableau illustrant les contenus de la section opaque du message LU1

4517A	Type :
4517B	Serveur - Date :
4517C	Version du logiciel :
4517D	Montant :
4517E	Instrument* :
4517F	Code :
4517G	Signature :

FIGURE 20A

Tableau illustrant le format du message LU2

45.105	[En-tête]
45.113A	Numéro d'identification :
45.113B	Transaction :
45.113C	Date :
45.113D	Service-catégorie :
45.117	Opaque :
45.150	[Queue]

FIGURE 20B

Tableau illustrant les contenus de la section opaque du message LU2

45.117A	Type :
45.117B	Serveur - Date :
45.117C	Montant :
45.117D	Réponse - Code :
45.117E	Méssage :
45.117F	Sévérité du logiciel :
45.117G	Message du logiciel :
45.117H	Honoraire :
45.117I	Balance :
45.117J	Session - Fonds :
45.117K	En-suspens :

FIGURE 21

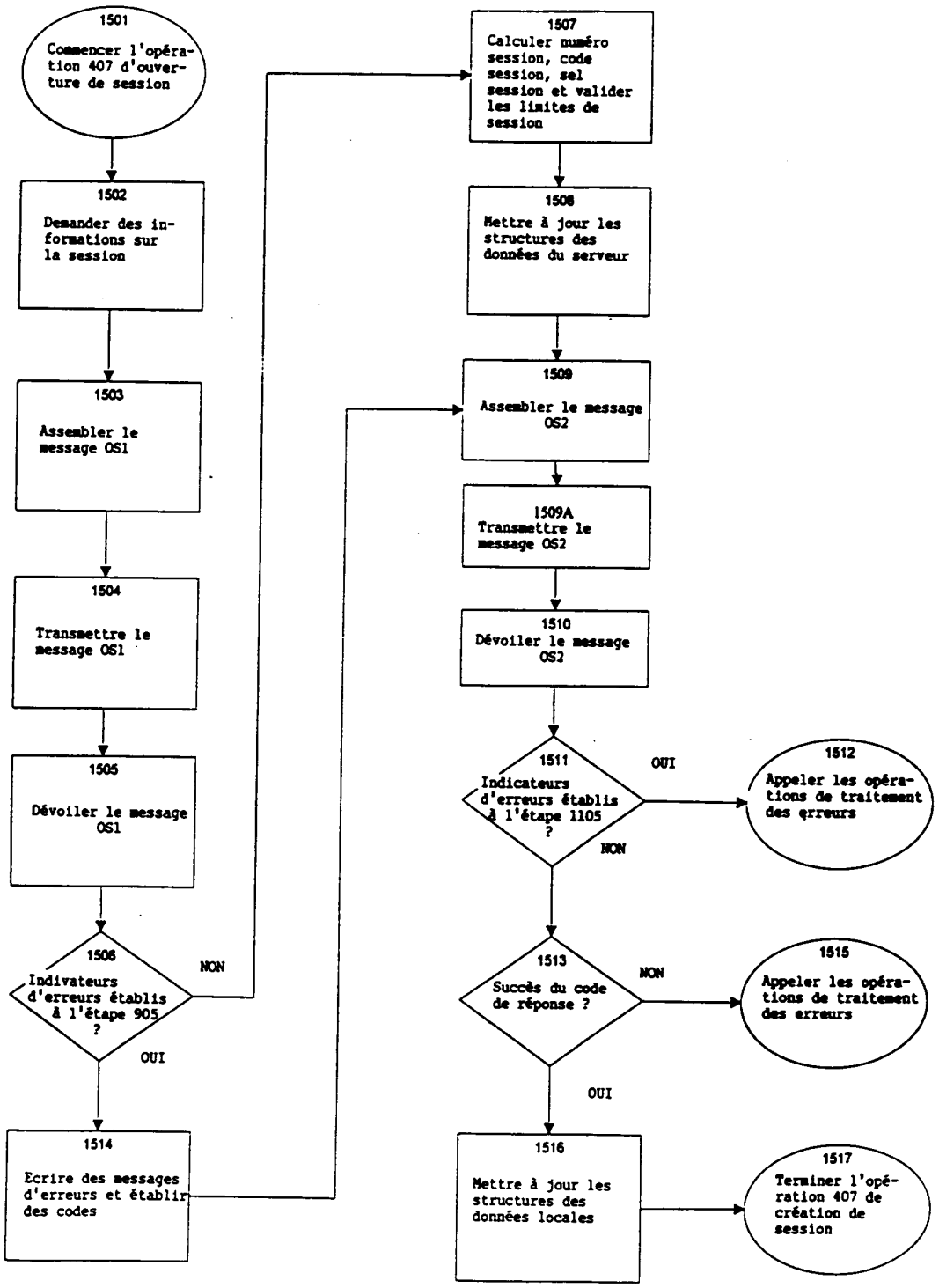

1501
Commencer l'opération 407 d'ouverture de session
1502
Demander des informations sur la session
1503
Assembler le message OS1
1504
Transmettre le message OS1
1505
Dévoiler le message OS1
1506
Indivateurs d'erreurs établis à l'étape 905 ?
NON
OUI
1514
Ecrire des messages d'erreurs et établir des codes
1507
Calculer numéro session, code session, sel session et valider les limites de session
1508
Mettre à jour les structures des données du serveur
1509
Assembler le message OS2
1509A
Transmettre le message OS2
1510
Dévoiler le message OS2
1511
Indicateurs d'erreurs établis à l'étape 1105 ?
OUI
NON
1512
Appeler les opérations de traitement des erreurs
1513
Succès du code de réponse ?
NON
OUI
1515
Appeler les opérations de traitement des erreurs
1516
Mettre à jour les structures des données locales
1517
Terminer l'opération 407 de création de session

FIGURE 22A

Tableau illustrant le format du message OS1

4605	[En-tête]
4613A	Numéro d'identification :
4613B	Transaction :
4613C	Date :
4613D	Code du serveur :
4613E	Service - Catégorie :
4617	Opaque :
4650	[Queue]

FIGURE 22B

Tableau illustrant les contenus de la section opaque du message OS1

4617A	Type :
4617B	Serveur - Date :
4617C	Version du logiciel :
4617D	Enregistrement - Note :
4617E	Montant :
4617F	Code - Durée de vie :
4617G	Code - Limite d'utilisation :
4617H	Code :
4617I	Signature :

FIGURE 23A

Tableau illustrant le format du message OS2

4705	[En-tête]
4713A	Numéro d'identification :
4713B	Transaction :
4713C	Date :
4713D	Service - Catégorie :
4717	Opaque :
4750	[Queue]

FIGURE 23B

Tableau illustrant les contenus de la section opaque du message OS2

4717A	Type :
4717B	Serveur - Date :
4717C	Réponse - Code :
4717D	Sévérité du logiciel :
4717E	Message du logiciel :
4717F	Message :
4717G	Code - Durée de vie
4717H	Code - Limite d'utilisation
4717I	Montant :
4717J	Change étranger :
4717K	Session - Fonds :
4717L	Balance :
4717M	En-suspens :
4717N	Honoraire :
4717O	Session - Numéro d'identification :
4717P	Session - Code :
4717Q	Session - Sel :

FIGURE 24A

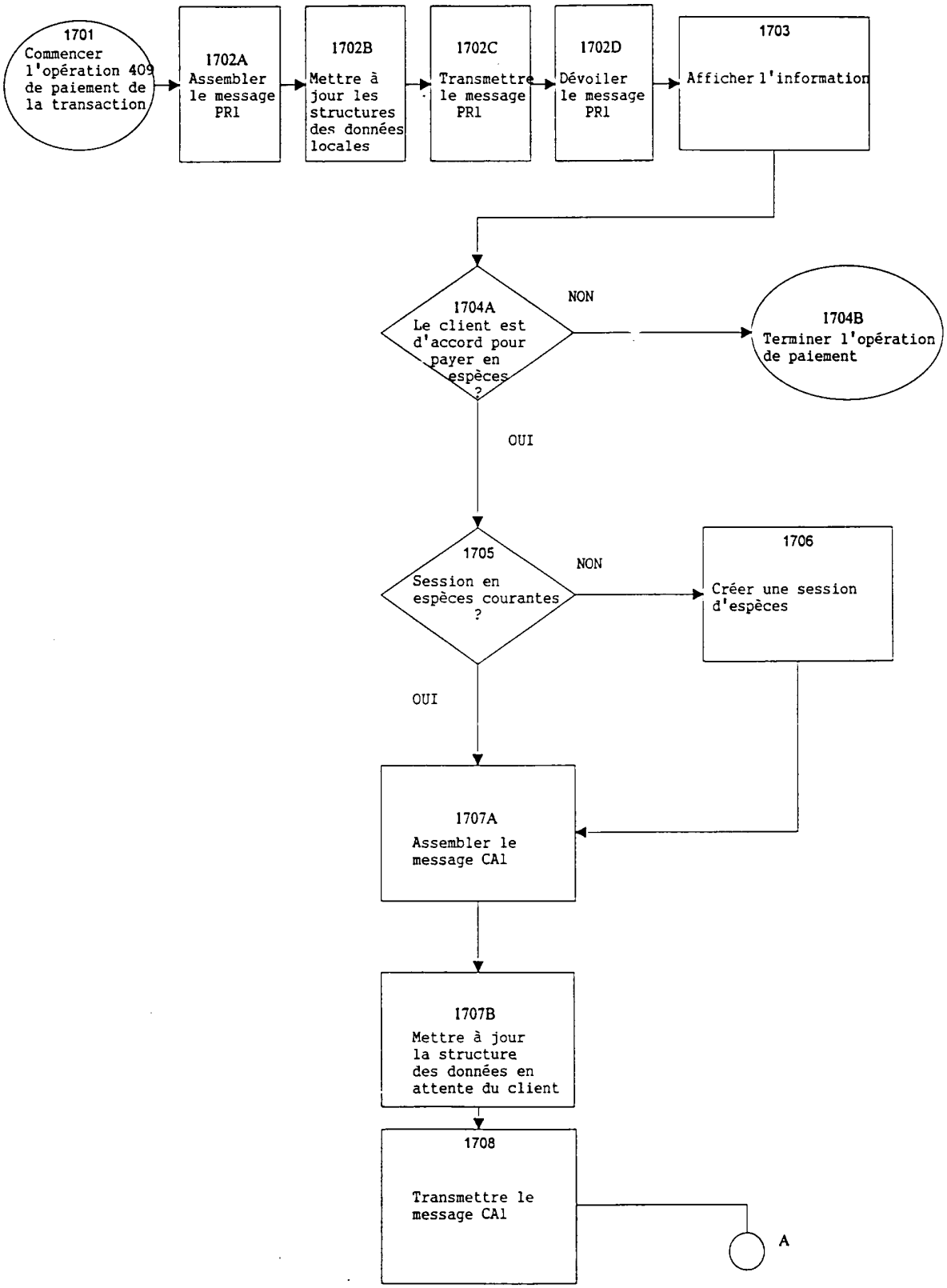

1701
Commencer l'opération 409 de paiement de la transaction
1702A
Assembler le message PR1
1702B
Mettre à jour les structures des données locales
1702C
Transmettre le message PR1
1702D
Dévoiler le message PR1
1703
Afficher l'information
1704A
Le client est d'accord pour payer en espèces ?
NON
1704B
Terminer l'opération de paiement
OUI
1705
Session en espèces courantes ?
NON
1706
Créer une session d'espèces
OUI
1707A
Assembler le message CA1
1707B
Mettre à jour la structure des données en attente du client
1708
Transmettre le message CA1
A

FIGURE 24B

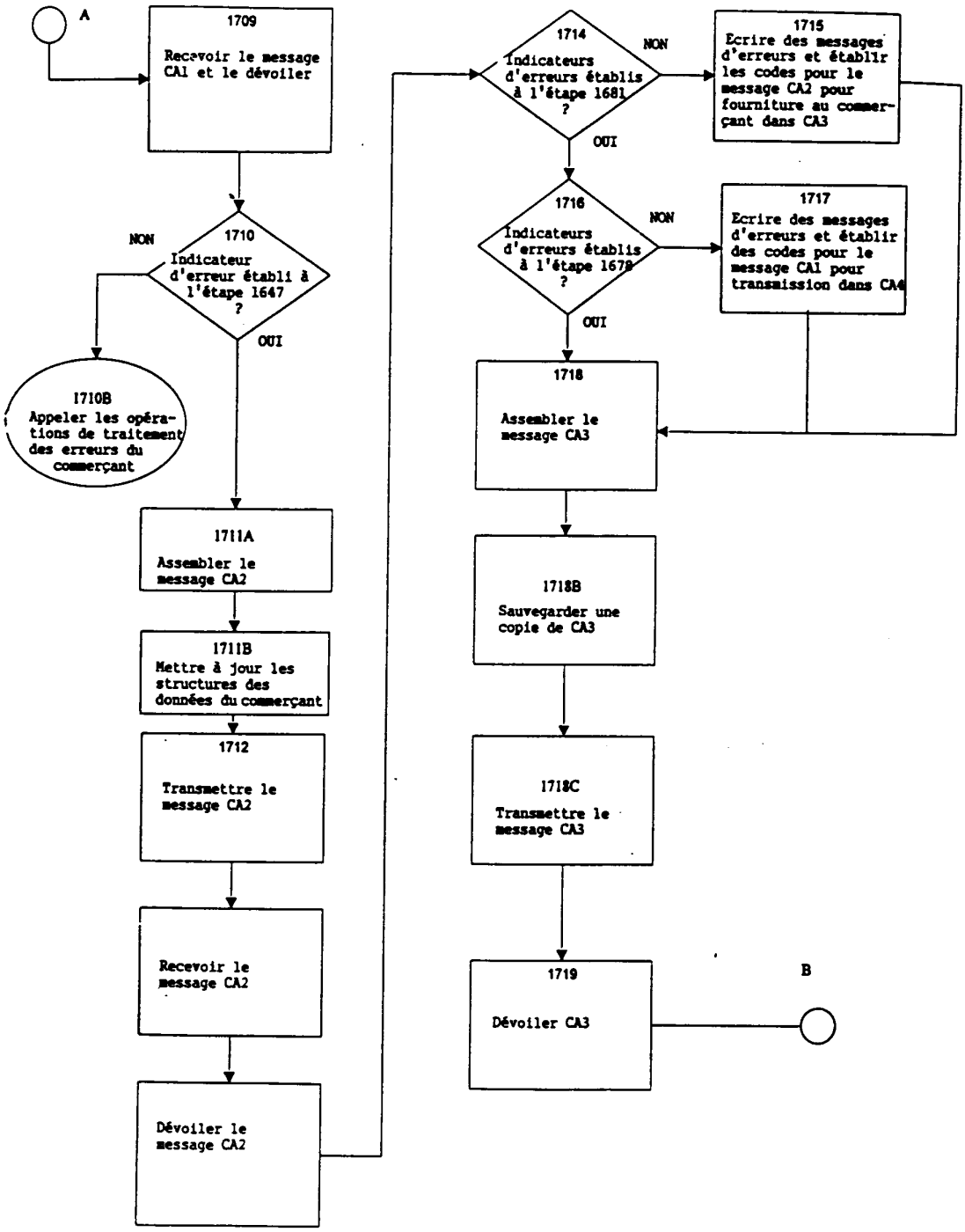

A
1709
Recevoir le message CA1 et le dévoiler
1710
Indicateur d'erreur établi à l'étape 1647 ?
NON
OUI
1710B
Appeler les opérations de traitement des erreurs du commerçant
1711A
Assembler le message CA2
1711B
Mettre à jour les structures des données du commerçant
1712
Transmettre le message CA2
Recevoir le message CA2
Dévoiler le message CA2
1714
Indicateurs d'erreurs établis à l'étape 1681 ?
NON
OUI
1715
Ecrire des messages d'erreurs et établir les codes pour le message CA2 pour fourniture au commerçant dans CA3
1716
Indicateurs d'erreurs établis à l'étape 1678 ?
NON
OUI
1717
Ecrire des messages d'erreurs et établir des codes pour le message CA1 pour transmission dans CA4
1718
Assembler le message CA3
1718B
Sauvegarder une copie de CA3
1718C
Transmettre le message CA3
1719
Dévoiler CA3
B

FIGURE 24C

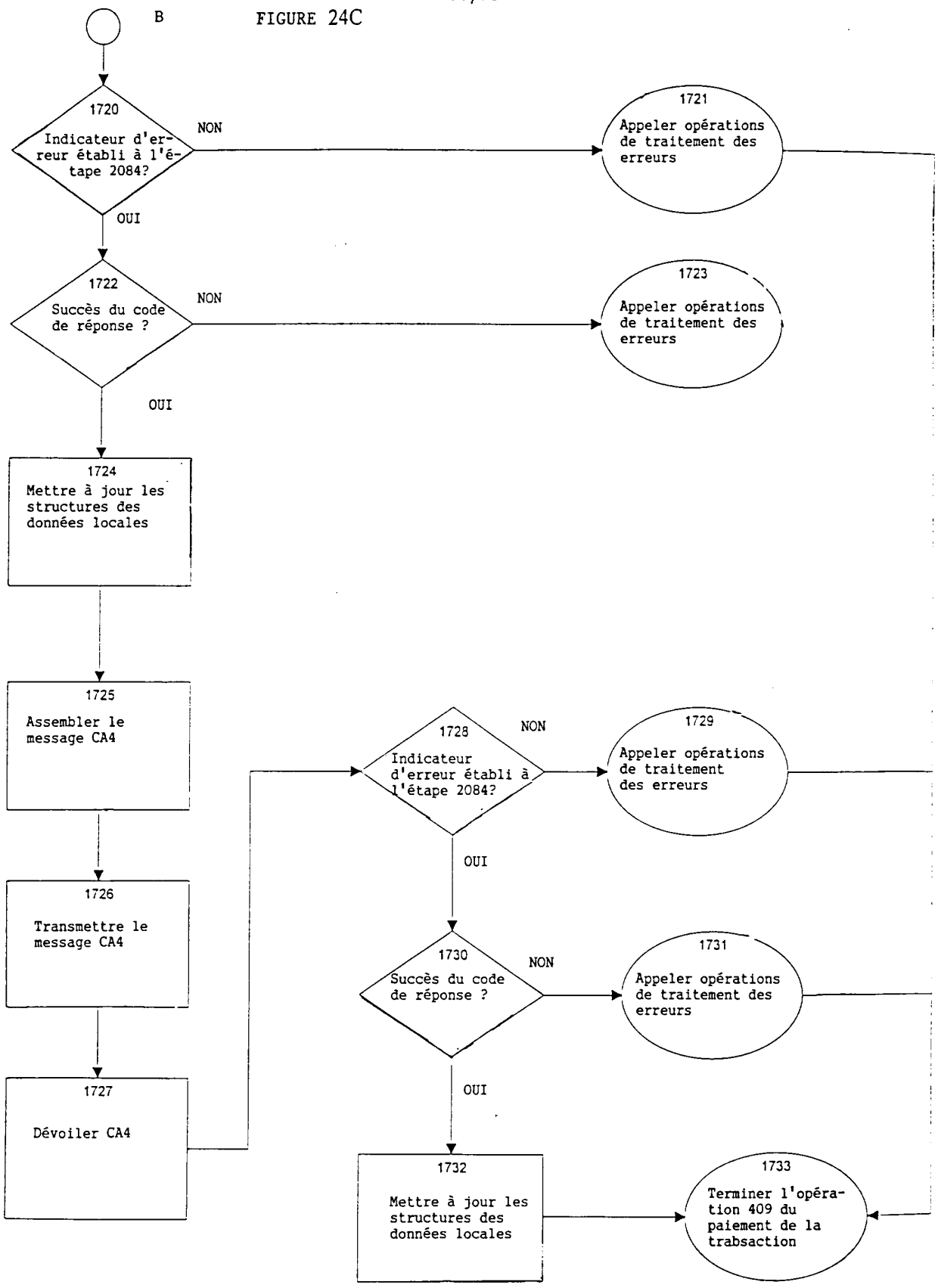

B
1720
Indicateur d'erreur établi à l'étape 2084?
NON
OUI
1721
Appeler opérations de traitement des erreurs
1722
Succès du code de réponse ?
NON
OUI
1723
Appeler opérations de traitement des erreurs
1724
Mettre à jour les structures des données locales
1725
Assembler le message CA4
1726
Transmettre le message CA4
1727
Dévoiler CA4
1728
Indicateur d'erreur établi à l'étape 2084?
NON
OUI
1729
Appeler opérations de traitement des erreurs
1730
Succès du code de réponse ?
NON
OUI
1731
Appeler opérations de traitement des erreurs
1732
Mettre à jour les structures des données locales
1733
Terminer l'opération 409 du paiement de la trabsaction

FIGURE 25

Tableau illustrant le format du message PR1

5005	[En-tête]
5013A	Type:
5013B	Commerçant - Numéro d'identification:
5013C	Commerçant - Ordre - Numéro d'identification:
5013D	Commerçant - Date
5013E	Commerçant - Version du logiciel:
5013F	Note:
5013G	Commerçant - Montant:
5013H	Acceptations:
5013I	RRU - Payer à:
5013J	RRU - Annulation:
5013K	RRU- Succès:
5013L	RRU - Echéc:
5013M	Commerçant - Signé - Contrôle de total de somme - Code:
5013N	Commerçant - Signé - Contrôle de total de somme - Code:
5013O	Commerçant - Montant 2:
5050	[Queue]

FIGURE 26

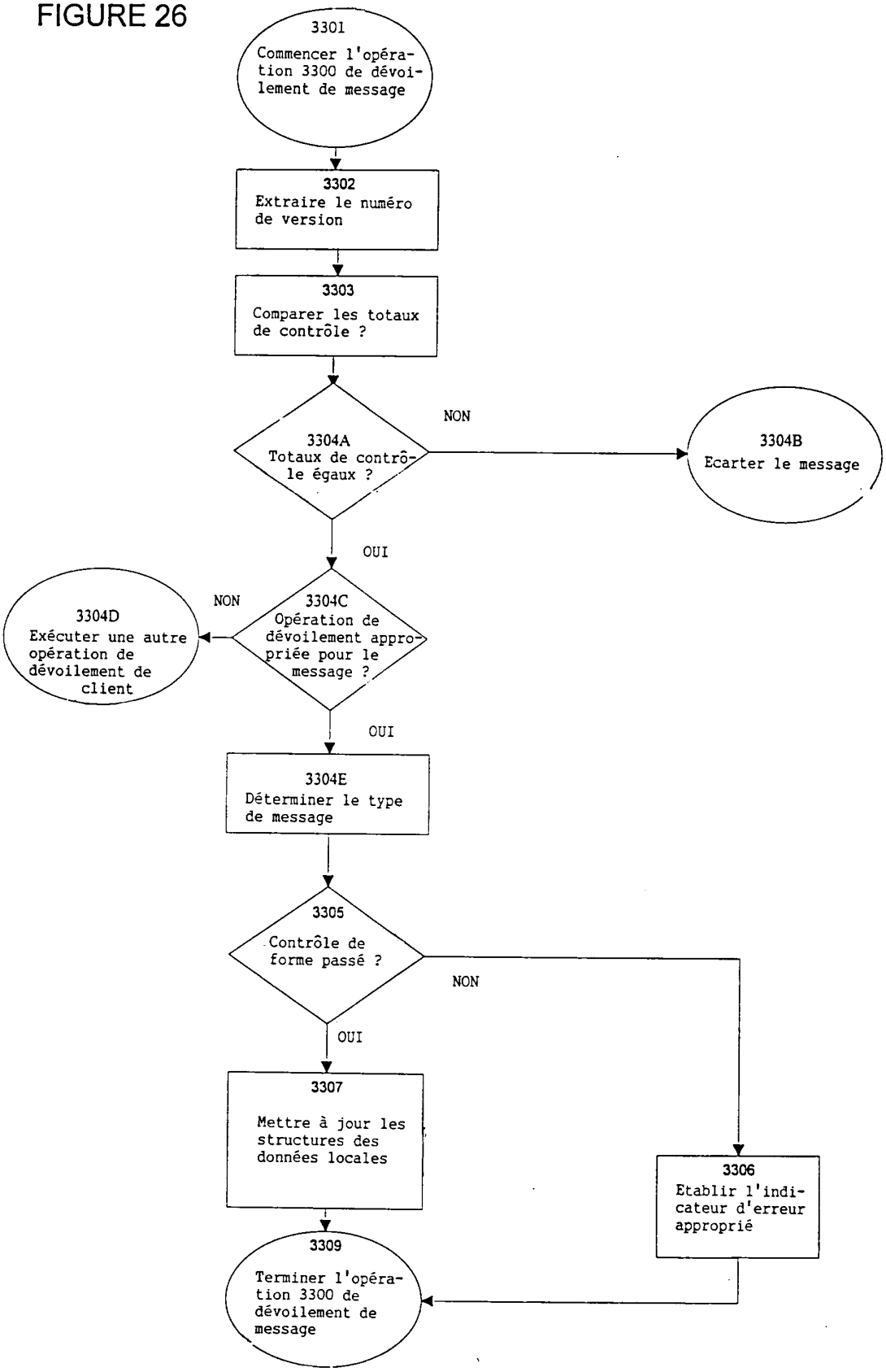

3301
Commencer l'opération 3300 de dévoilement de message
3302
Extraire le numéro de version
3303
Comparer les totaux de contrôle ?
3304A
Totaux de contrôle égaux ?
NON
3304B
Ecarter le message
OUI
3304C
Opération de dévoilement appropriée pour le message ?
NON
3304D
Exécuter une autre opération de dévoilement de client
OUI
3304E
Déterminer le type de message
3305
Contrôle de forme passé ?
NON
OUI
3307
Mettre à jour les structures des données locales
3306
Etablir l'indicateur d'erreur approprié
3309
Terminer l'opération 3300 de dévoilement de message

FIG. 27

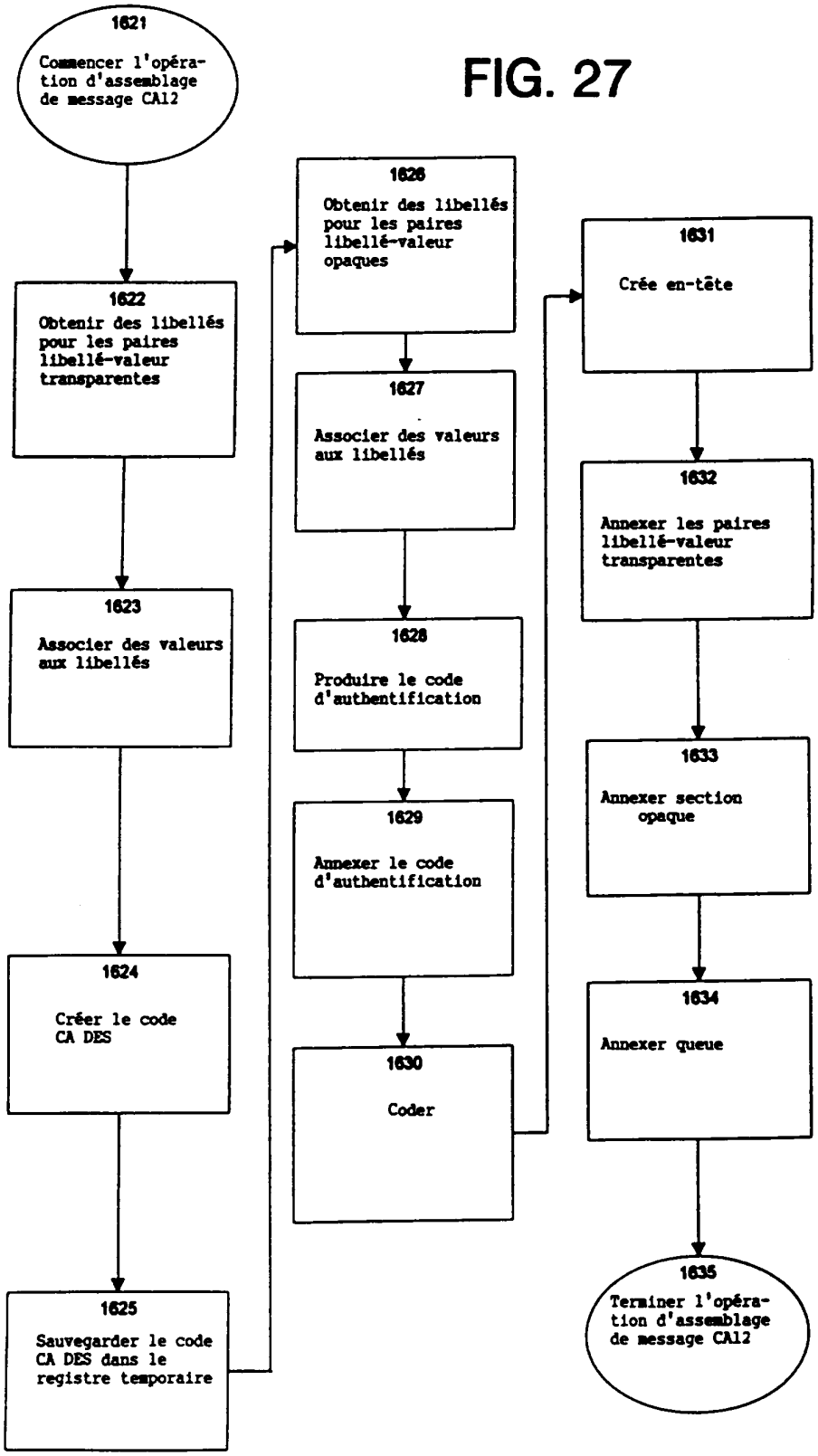

1621
Commencer l'opération d'assemblage de message CA12
1622
Obtenir des libellés pour les paires libellé-valeur transparentes
1623
Associer des valeurs aux libellés
1624
Créer le code CA DES
1625
Sauvegarder le code CA DES dans le registre temporaire
1626
Obtenir des libellés pour les paires libellé-valeur opaques
1627
Associer des valeurs aux libellés
1628
Produire le code d'authentification
1629
Annexer le code d'authentification
1630
Coder
1631
Crée en-tête
1632
Annexer les paires libellé-valeur transparentes
1633
Annexer section opaque
1634
Annexer queue
1635
Terminer l'opération d'assemblage de message CA12

FIGURE 28A

Tableau illustrant le format du message CA1

5105	[En-tête]
5113A	Type:
5113B	Version:
5113C	Session - Numéro d'identification:
5113D	Indice:
5113	Bénéficiaire - Devise:
5113F	Note - Contrôle de total de somme:
5113G	Bénéficiaire - Numéro d'identification:
5113H	Ordre - Numéro d'identification:
5113I	Service - Catégorie:
5117	Opaque:
5150	[Queue]

FIGURE 28B

Tableau illustrant les contenus de la section opaque du message CA1

5117A	Montant:
5117B	Authentification - Code:

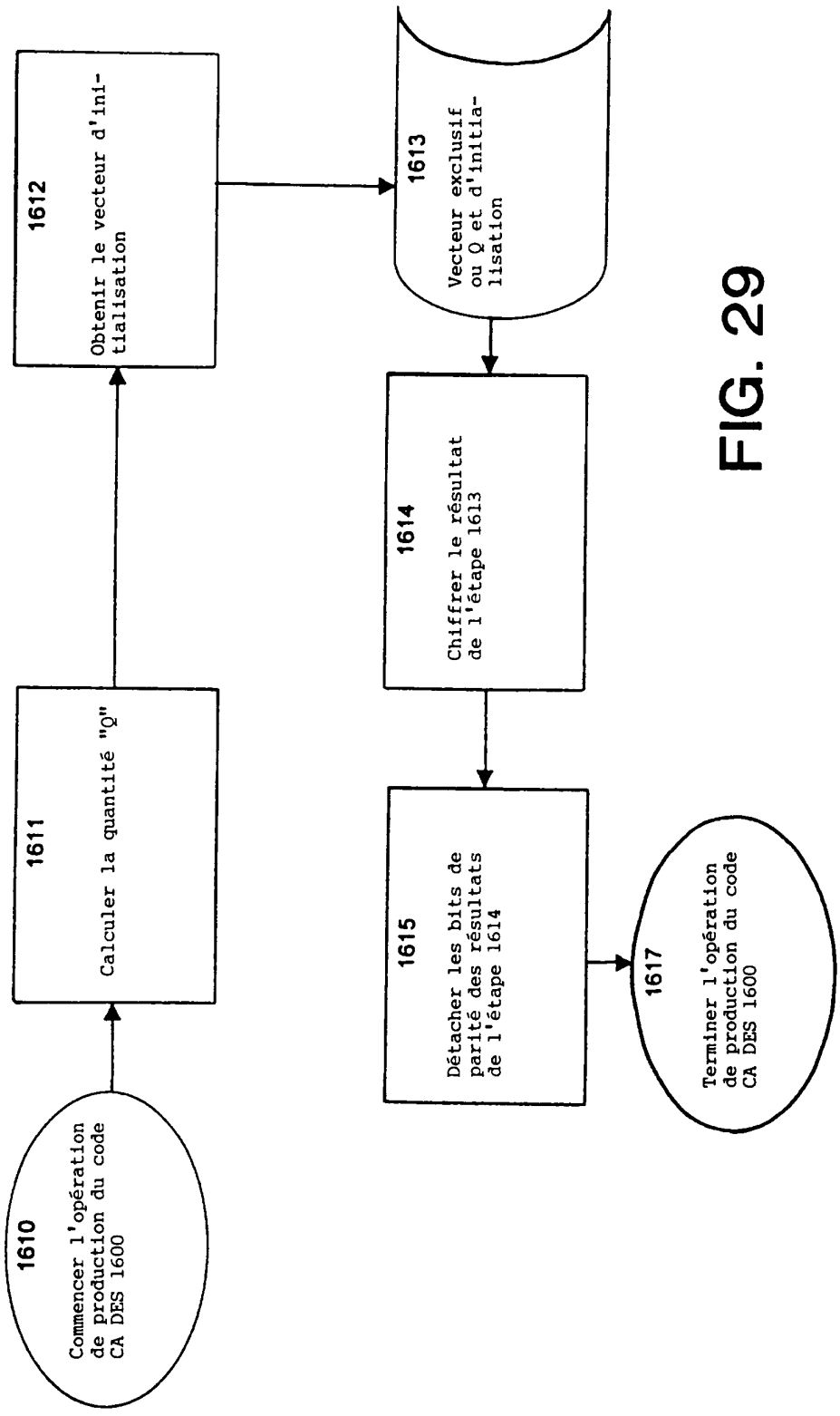

1610
Commencer l'opération de production du code CA DES 1600
1611
Calculer la quantité "Q"
1612
Obtenir le vecteur d'initialisation
1613
Vecteur exclusif ou Q et d'initialisation
1614
Chiffrer le résultat de l'étape 1613
1615
Détacher les bits de parité des résultats de l'étape 1614
1617
Terminer l'opération de production du code CA DES 1600

FIG. 29

FIIGURE 30

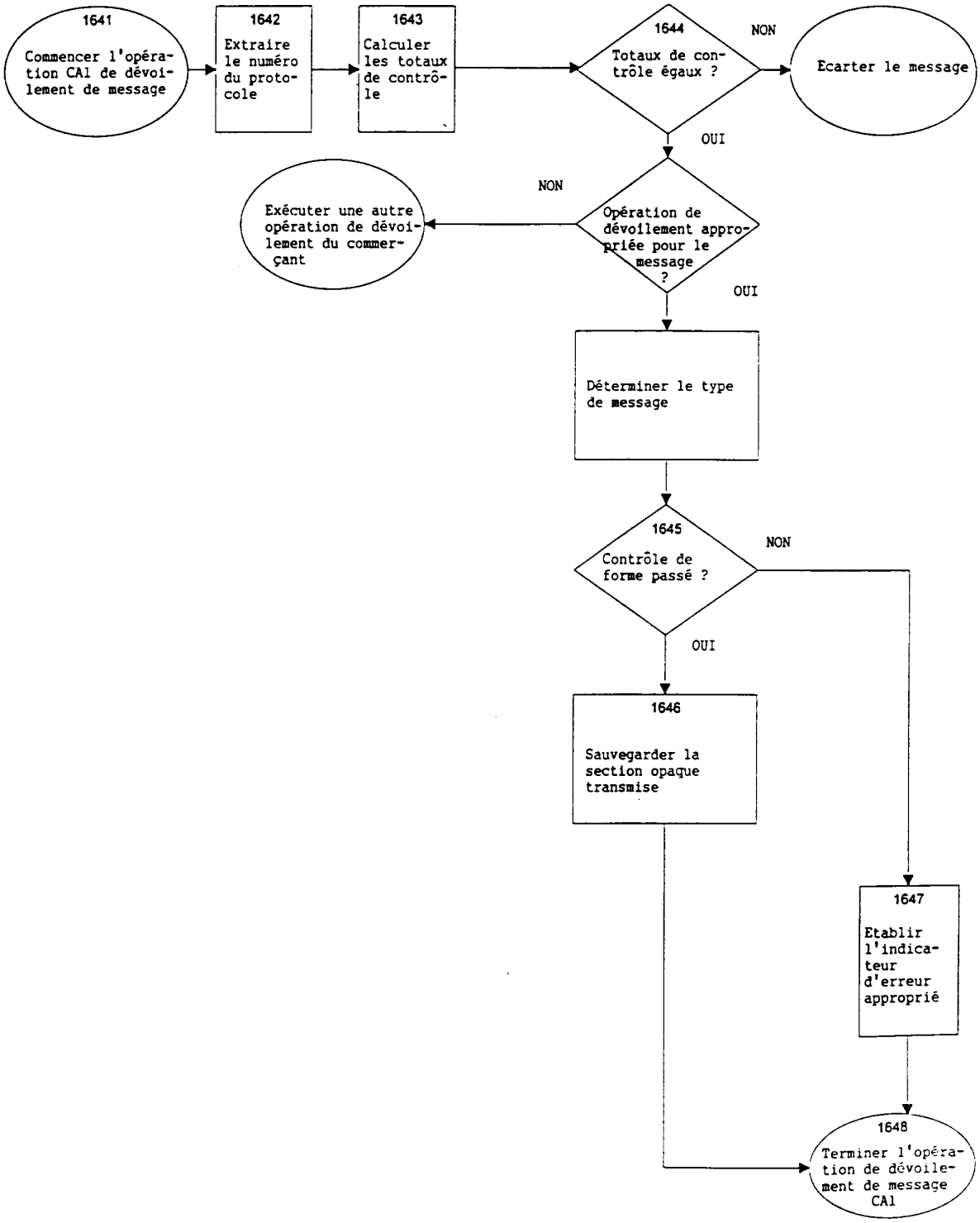

1641
Commencer l'opération CA1 de dévoilement de message
1642
Extraire le numéro du protocole
1643
Calculer les totaux de contrôle
1644
Totaux de contrôle égaux ?
NON
Ecarter le message
OUI
NON
Exécuter une autre opération de dévoilement du commerçant
Opération de dévoilement appropriée pour le message ?
OUI
Déterminer le type de message
1645
Contrôle de forme passé ?
NON
OUI
1646
Sauvegarder la section opaque transmise
1647
Etablir l'indicateur d'erreur approprié
1648
Terminer l'opération de dévoilement de message CA1

FIGURE 31A

Tableau illustrant le format du message CA2

5205	[En-tête]
5213A	Type:
5213B	Version:
5213C	Session - Numéro d'identification:
5213D	Indice:
5210E	Service - Catégorie:
5217.1	Commerçant - Opaque:
5217.2	Client - Opaque:
5250	[Queue]

FIGURE 31B

Tableau illustrant les contenus de la section opaque du message CA2

5217.1A	Type:
5217.1B	Version:
5217.1C	Type:
5217.1D	Sous-version:
5217.1E	Payeur - Session - Numéro d'identification$_n$:
5217.1F	Payeur - Indice$_n$:
5217.1G	Note - Contrôle$_n$ de total de somme:
5217.1H	Bénéficiaire - Numéro d'identification$_n$:
5217.1I	Ordre - Numéro d'identification$_n$:
5217.1J	Commerçant - Montant$_n$:
5217.1K	Authentification - Code:

FIGURE 31C

Tableau illustrant les contenus de la paire libellé-valeur 5217.2

5217.2A	Montant:
5217.2B	Authentification - Code:

FIGURE 32A

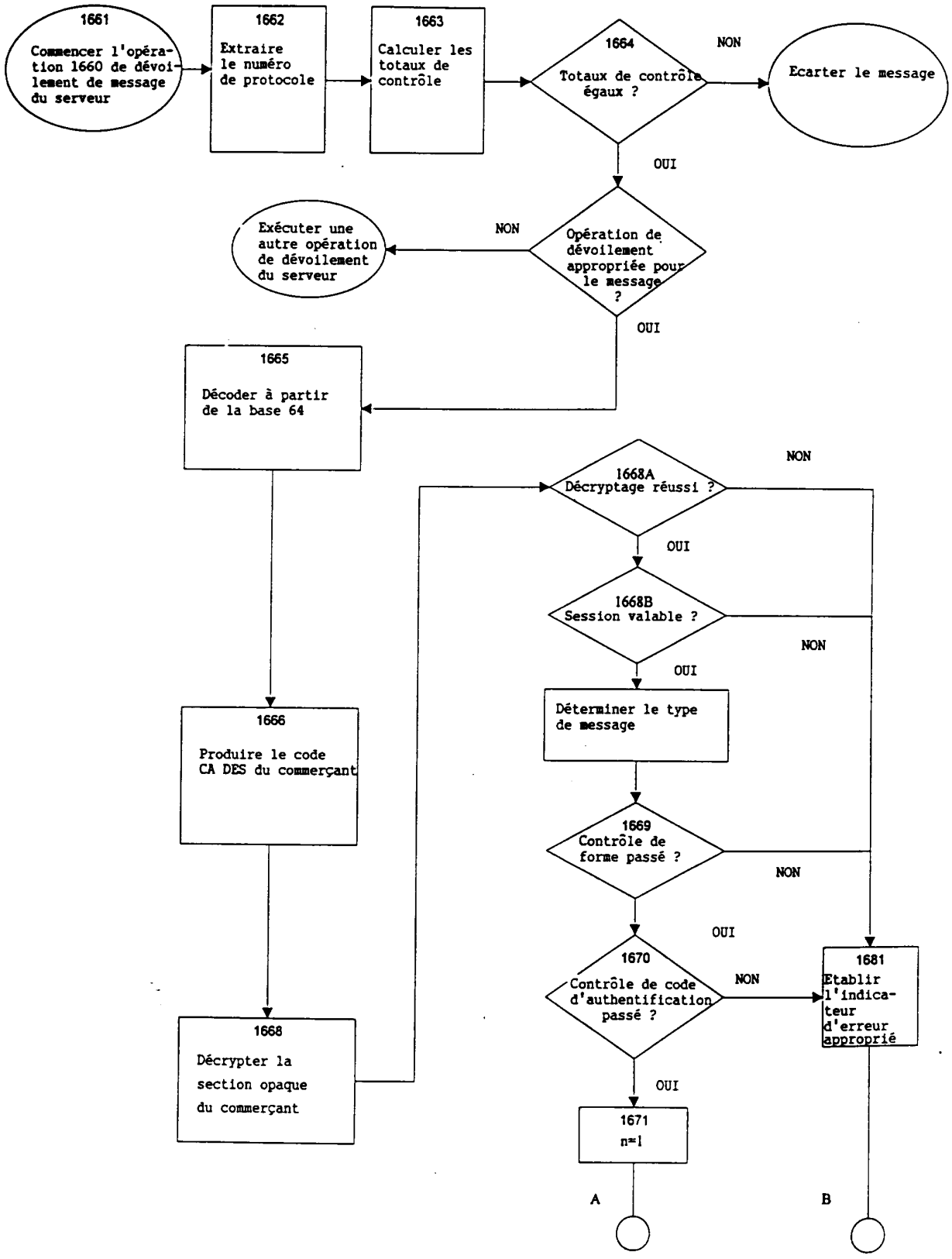

1661
Commencer l'opération 1660 de dévoilement de message du serveur
1662
Extraire le numéro de protocole
1663
Calculer les totaux de contrôle
1664
Totaux de contrôle égaux ?
NON
Ecarter le message
OUI
Opération de dévoilement appropriée pour le message ?
NON
Exécuter une autre opération de dévoilement du serveur
OUI
1665
Décoder à partir de la base 64
1666
Produire le code CA DES du commerçant
1668
Décrypter la section opaque du commerçant
1668A
Décryptage réussi ?
NON
OUI
1668B
Session valable ?
NON
OUI
Déterminer le type de message
1669
Contrôle de forme passé ?
NON
OUI
1670
Contrôle de code d'authentification passé ?
NON
OUI
1681
Etablir l'indicateur d'erreur approprié
1671
n=1
A
B

FIGURE 32B

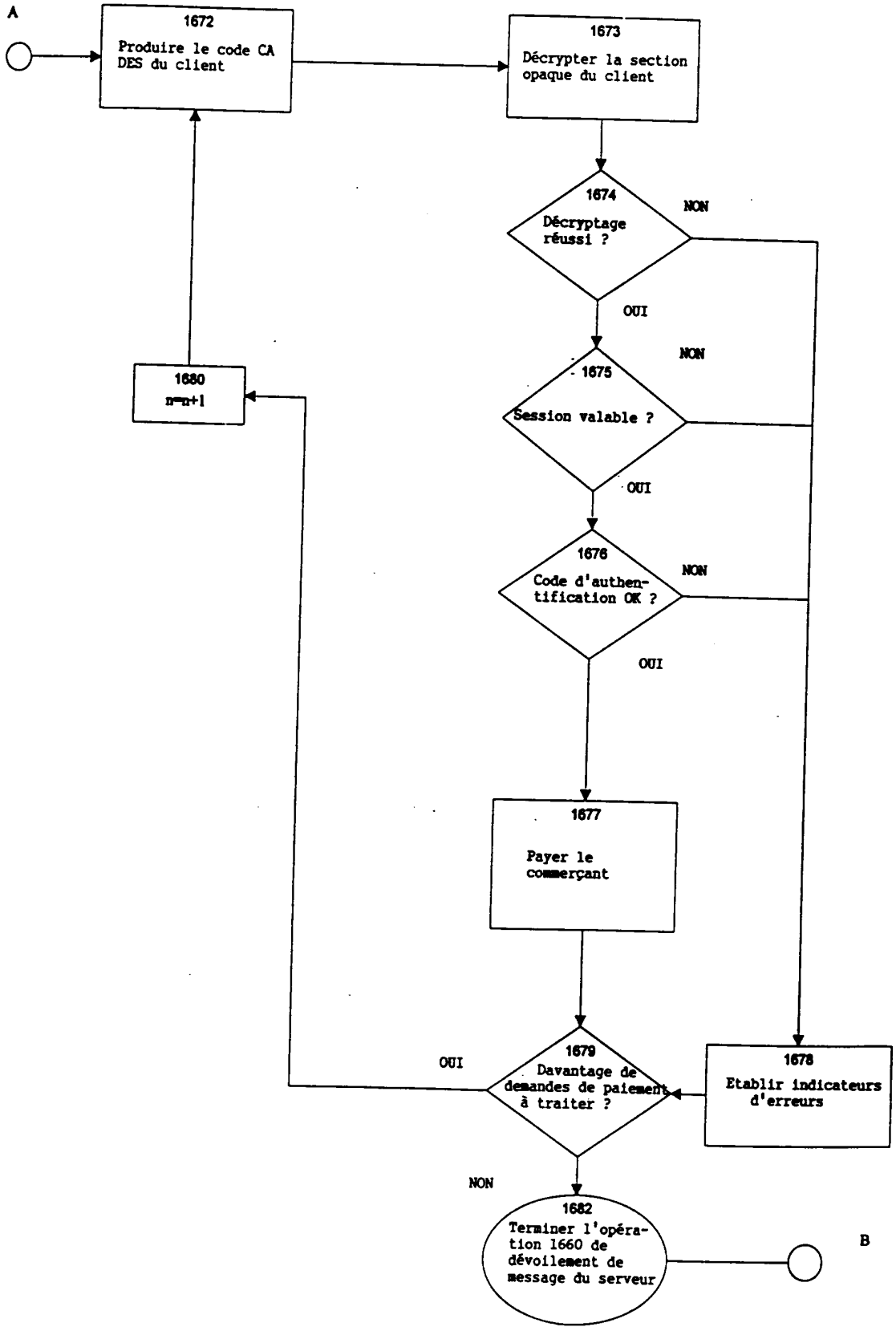

A
1672
Produire le code CA DES du client
1673
Décrypter la section opaque du client
1674
Décryptage réussi ?
NON
OUI
1675
Session valable ?
NON
OUI
1676
Code d'authentification OK ?
NON
OUI
1677
Payer le commerçant
1678
Etablir indicateurs d'erreurs
1679
Davantage de demandes de paiement à traiter ?
OUI
NON
1680
n=n+1
1682
Terminer l'opération 1660 de dévoilement de message du serveur
B

FIGURE 33

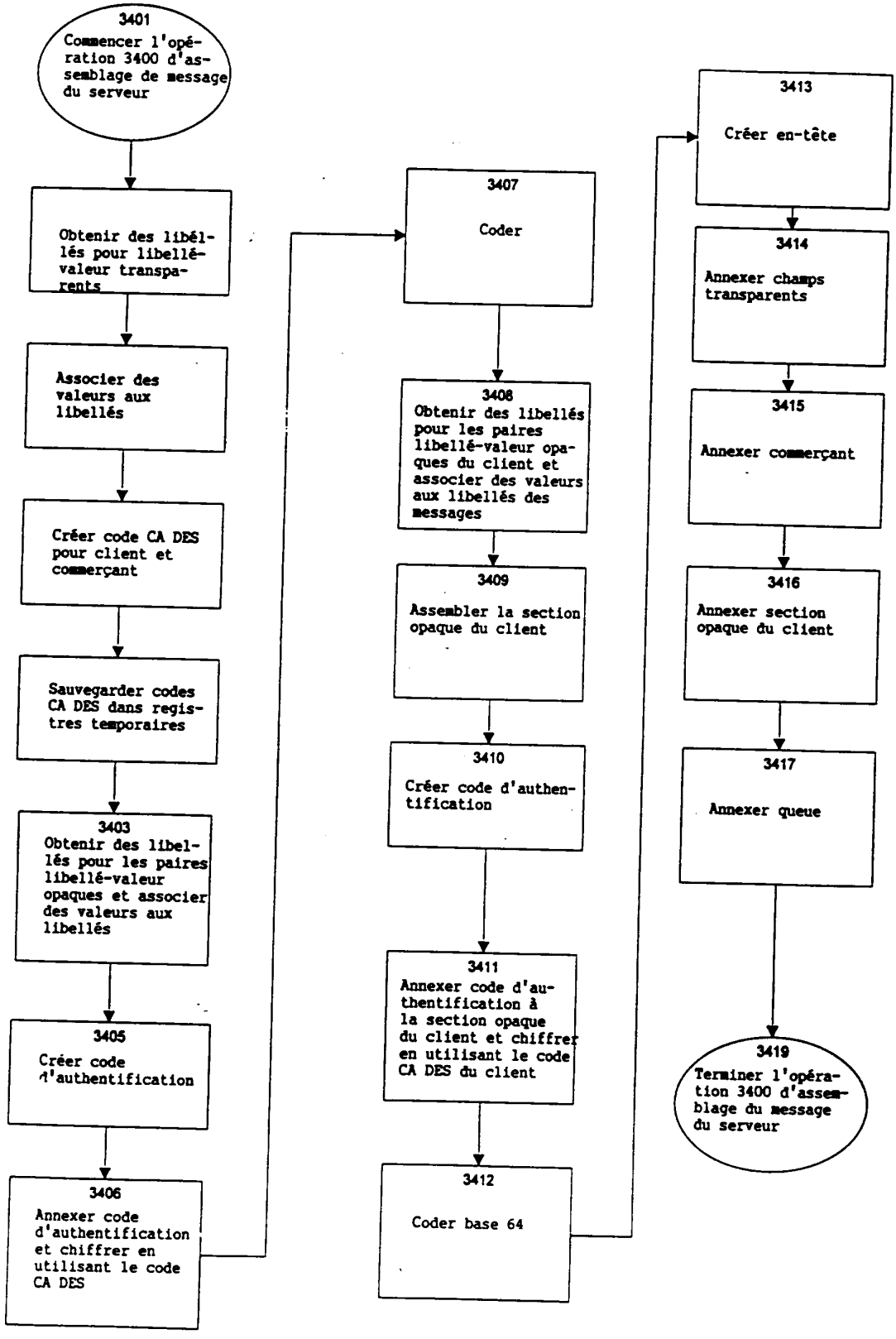

3401
Commencer l'opération 3400 d'assemblage de message du serveur
Obtenir des libéllés pour libellé-valeur transparents
Associer des valeurs aux libellés
Créer code CA DES pour client et commerçant
Sauvegarder codes CA DES dans registres temporaires
3403
Obtenir des libellés pour les paires libellé-valeur opaques et associer des valeurs aux libellés
3405
Créer code d'authentification
3406
Annexer code d'authentification et chiffrer en utilisant le code CA DES
3407
Coder
3408
Obtenir des libellés pour les paires libellé-valeur opaques du client et associer des valeurs aux libellés des messages
3409
Assembler la section opaque du client
3410
Créer code d'authentification
3411
Annexer code d'authentification à la section opaque du client et chiffrer en utilisant le code CA DES du client
3412
Coder base 64
3413
Créer en-tête
3414
Annexer champs transparents
3415
Annexer commerçant
3416
Annexer section opaque du client
3417
Annexer queue
3419
Terminer l'opération 3400 d'assemblage du message du serveur

FIGURE 34A

Tableau illustrant le format du message CA3

5305	[En-tête]
5313A	Type:
5313B	Version:
5313C	Session - Numéro d'identification:
5313D	Indice:
5313E	Service - Catégorie:
5317.1	Commerçant - Section opaque:
5317.2	Client - Section opaque:
5350	[Queue]

FIGURE 34B

Tableau illustrant les contenus de la section opaque du message CA3

5317.1A	Sous-type:
5317.1B	Sous-version:
5317.1C	Réponse - Code:
5317.1D	Honoraire:
5317.1E	Problème:
5317.1F	Remarque:
5317.1G	Sous-type$_n$:
5317.1H	Sous-version$_n$:
5317.1I	Payeur - Session - Numéro d'identification$_n$:
5317.J	Payeur - Indice$_n$:
5317.1K	Réponse - Code$_n$:
5317.1L	Remarque:
5317.1M	Montant recueilli:
5317.1N	Problème$_n$:
5317.1O	Ordre - Numéro d'identification$_n$:
5317.1P	Demande - Version:
5317.1Q	Code d'authetification:

FIGURE 34C

Tableau illustrant les contenus de la paire libellé-valeur 5317.2

5317.2A	Réponse - Code:
5317.2B	Remarque:
5317.2C	Change étranger:
5317.2D	Montant:
5317.2E	Problème:
5317.2F	Ordre - Numéro d'identification:
5317.2G	Demande - Version:
5317.2H	Code d'authentification:

FIGURE 35

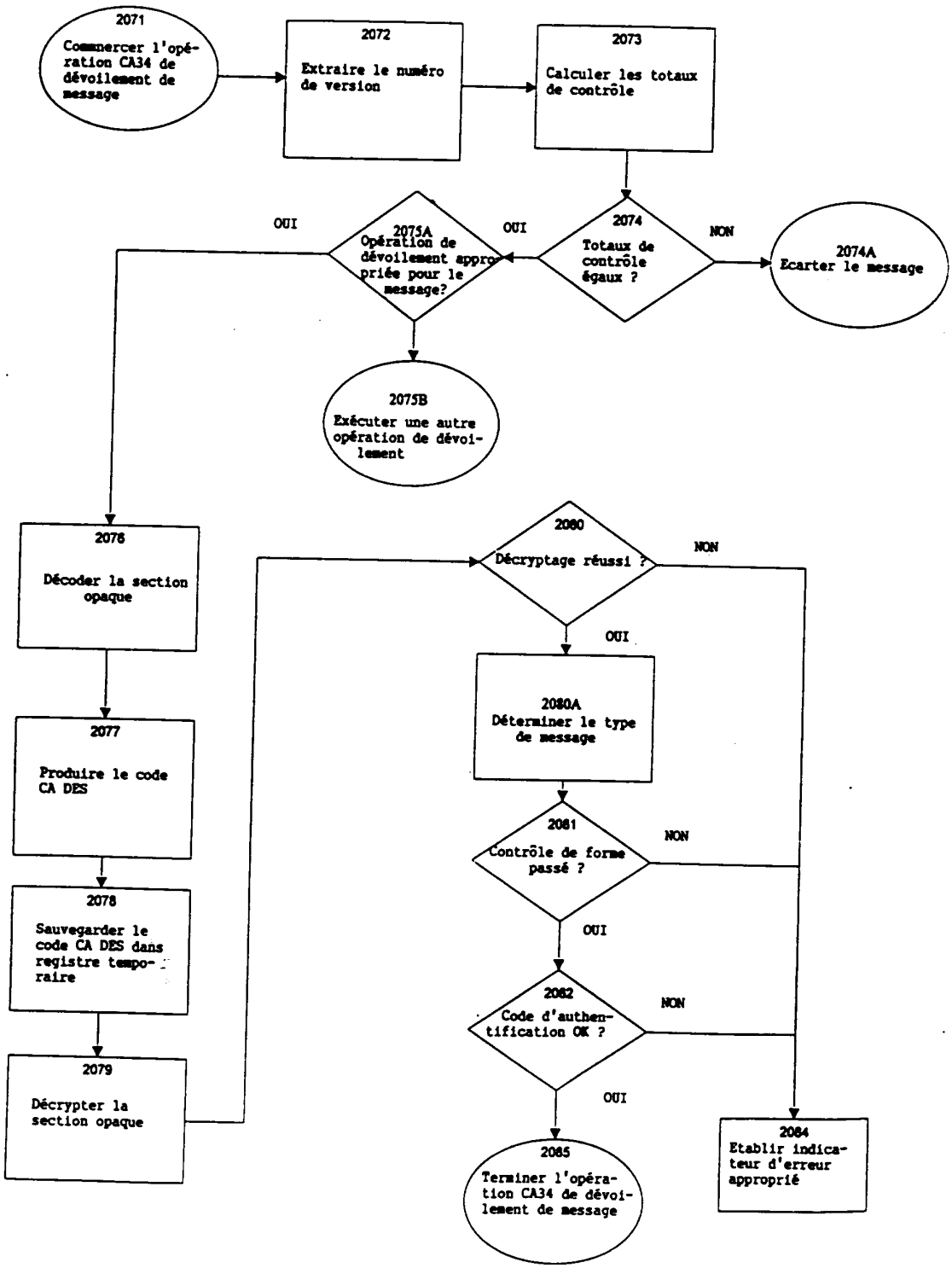

2071
Commencer l'opération CA34 de dévoilement de message
2072
Extraire le numéro de version
2073
Calculer les totaux de contrôle
2074
Totaux de contrôle égaux ?
NON
2074A
Ecarter le message
OUI
2075A
Opération de dévoilement appropriée pour le message?
OUI
2075B
Exécuter une autre opération de dévoilement
2076
Décoder la section opaque
2077
Produire le code CA DES
2078
Sauvegarder le code CA DES dans registre temporaire
2079
Décrypter la section opaque
2080
Décryptage réussi ?
NON
OUI
2080A
Déterminer le type de message
2081
Contrôle de forme passé ?
NON
OUI
2082
Code d'authentification OK ?
NON
OUI
2084
Etablir indicateur d'erreur approprié
2085
Terminer l'opération CA34 de dévoilement de message

FIG. 36

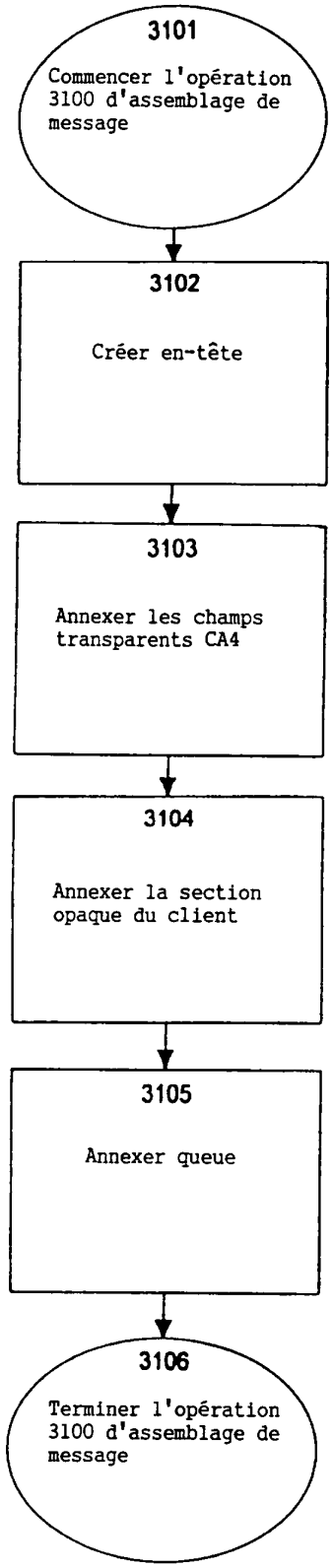

3101
Commencer l'opération 3100 d'assemblage de message
3102
Créer en-tête
3103
Annexer les champs transparents CA4
3104
Annexer la section opaque du client
3105
Annexer queue
3106
Terminer l'opération 3100 d'assemblage de message

FIGURE 37A

Tableau illustrant le format du message CA4

5405	[En-tête]
5413A	Type:
5413B	Version:
5413C	Session - Numéro d'identification:
5413D	Indice:
5413F	Ordre - Numéro d'identification:
5413G	Service - Catégorie:
5417	Opaque:
5450	[Queue]

FIGURE 37B

Tableau illustrant les contenus de la section opaque du message CA4

5417A	Réponse - Code:
5417B	Remarque:
5417C	Change étranger:
5417D	Montant:
5417E	Problème:
5417F	Ordre - Numéro d'identification:
5417G	Service - Catégorie:
5417H	Code d'authentification:

FIGURE 38

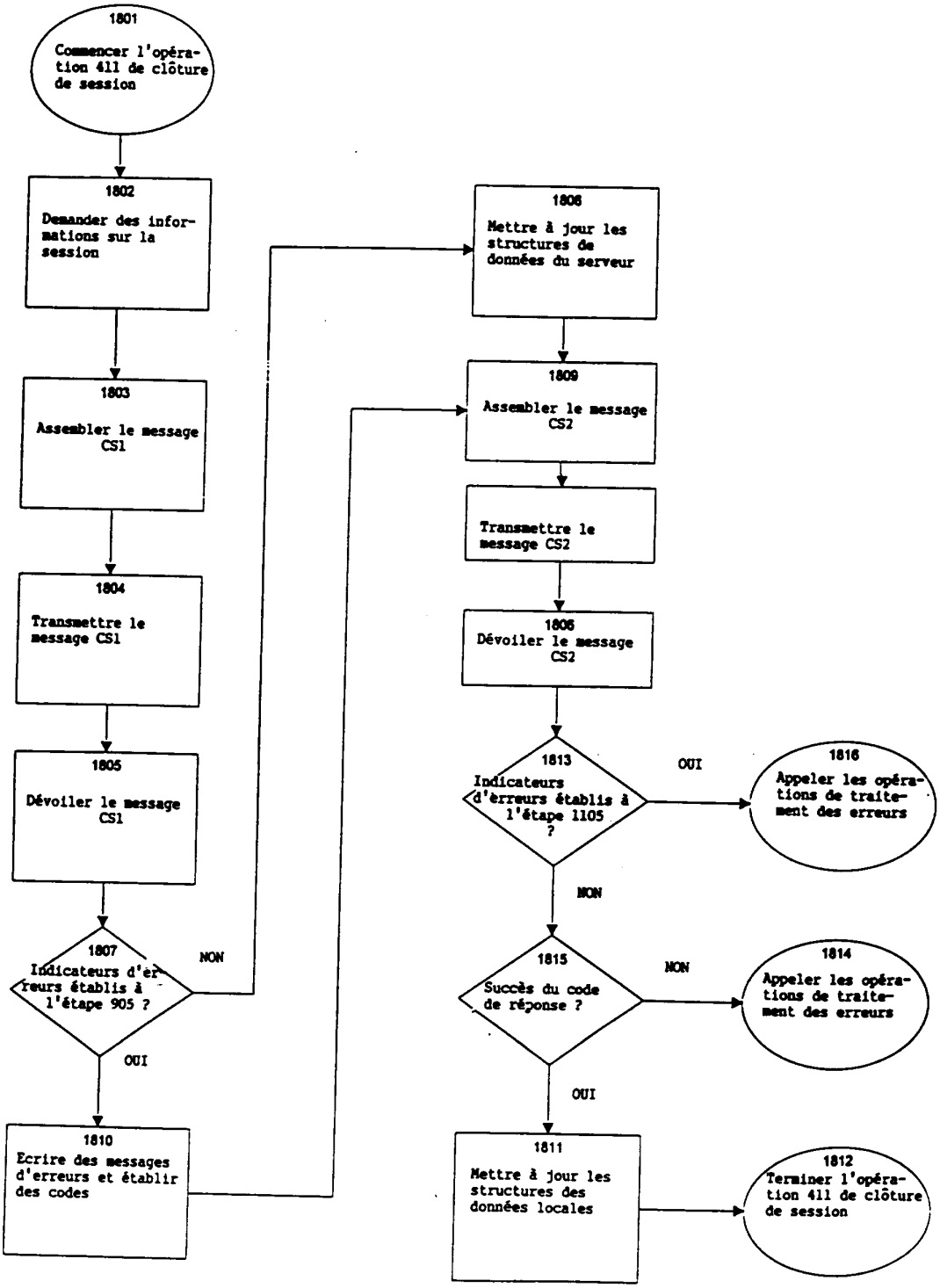

1801
Commencer l'opération 411 de clôture de session
1802
Demander des informations sur la session
1803
Assembler le message CS1
1804
Transmettre le message CS1
1805
Dévoiler le message CS1
1807
Indicateurs d'erreurs établis à l'étape 905 ?
NON
OUI
1810
Ecrire des messages d'erreurs et établir des codes
1806
Mettre à jour les structures de données du serveur
1809
Assembler le message CS2
Transmettre le message CS2
1808
Dévoiler le message CS2
1813
Indicateurs d'erreurs établis à l'étape 1105 ?
OUI
1816
Appeler les opérations de traitement des erreurs
NON
1815
Succès du code de réponse ?
NON
1814
Appeler les opérations de traitement des erreurs
OUI
1811
Mettre à jour les structures des données locales
1812
Terminer l'opération 411 de clôture de session

FIGURE 39A

Tableau illustrant le format du message CS1

4805	[En-tête]
4813A	Numéro d'identification:
4813B	Transaction:
4813C	Date:
4813D	Code du serveur:
4813E	Service - Catégorie:
4817	Opaque:
4850	[Queue]

FIGURE 39B

Tableau illustrant les contenus de la section opaque du message CS1

4817A	Type:
4817B	Serveur - Date:
4817C	Version de logiciel:
4817D	Enregistrement - Note:
4817E	Session - Numéro d'identification:
4817F	Demande - Journal:
4817G	Code:
4817H	Signature:

FIGURE 40A

Tableau illustrant le format du message CS2

4905	[En-tête]
4913A	Numéro d'identification:
4913B	Transaction:
4913C	Date:
4913D	Service - Catégorie:
4917	Opaque:
4950	[Queue]

FIGURE 40B

Tableau illustrant les contenus de la section opaque du message CS2

4917A	Type:
4917B	Serveur - Date:
4917C	Réponse - Code:
4917D	Sévérité du logiciel:
4917E	Message du logiciel:
4917F	Message:
4917G	Honoraire:
4917H	Montant: