(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

PCT

(43) Date de la publication internationale
16 novembre 2006 (16.11.2006)

(10) Numéro de publication internationale
WO 2006/120364 A2

(51) Classification internationale des brevets : Non classée

(21) Numéro de la demande internationale :
PCT/FR2006/050403

(22) Date de dépôt international : 28 avril 2006 (28.04.2006)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0551239 12 mai 2005 (12.05.2005) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6 Place d'Alleray, F-75015 Paris (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : **MACARIO-RAT, Gilles** [FR/FR]; 108 avenue Victor Hugo, F-92170 Vanves (FR).

(74) Mandataire : **LAPOUX, Roland**; CABINET MARTINET & LAPOUX, 43 boulevard Vauban - BP 405 Guyancourt, F-78055 Saint Quentin Yvelines Cedex (FR).

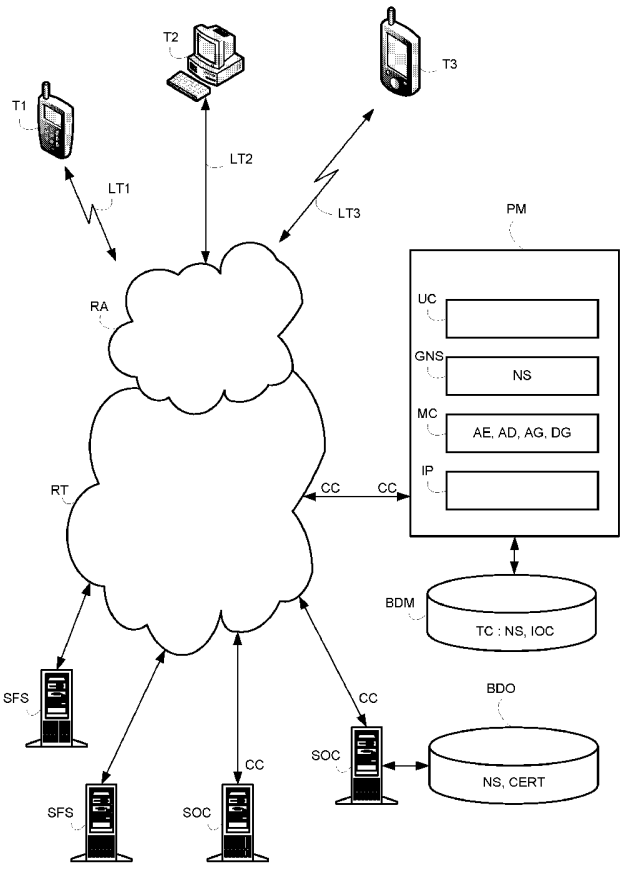
(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH,

[Suite sur la page suivante]

(54) **Title:** TRANSMISSION OF A PREPAID CARD CODE TO A CARD OPERATOR SERVER

(54) **Titre :** TRANSFERT D'UN CODE DE CARTE PREPAYEE VERS UN SERVEUR D'OPERATEUR DE CARTES



(57) **Abstract:** The invention relates to a method for transmitting confidential codes (CC) assigned to respective prepaid cards from a user's terminals (T) to a card operator servers (SOC) via a mediation platform (PM) consisting, prior to using cards, in distributing the serial numbers assigned to the prepaid cards in transmitting tables by means of the platform and in assigning the operator server addresses to said tables. When a card is used, the platform receiving the confidential code deducts the serial number therefrom for reading the operator server address and transmits said confidential code to an operator server which is indicated in said address.

(57) **Abrégé :** Pour transférer des codes confidentiels (CC) respectivement associés à des cartes prépayées depuis des terminaux d'utilisateur (T) vers des serveurs d'opérateur de cartes (SOC) via une plateforme de médiation (PM), avant l'utilisation des cartes la plateforme répartit des numéros de série respectivement associés à des cartes prépayées dans des tables de correspondance et associe des adresses de serveurs d'opérateurs respectivement aux tables. Lors de l'utilisation d'une carte, la plateforme recevant un code confidentiel en déduit le numéro de série, recherche la table de correspondance incluant le numéro de série déduit afin d'y lire l'adresse de serveur d'opérateur, et transmet le code confidentiel au serveur d'opérateur désigné par ladite adresse.

WO 2006/120364 A2

GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

— *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii))*

— *relative à la qualité d'inventeur (règle 4.17.iv))*

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

Transfert d'un code de carte prépayée vers un serveur d'opérateur de cartes

La présente invention concerne un transfert d'un code confidentiel associé à une carte prépayée virtuelle depuis un terminal d'utilisateur vers un serveur d'opérateur de cartes gérant ladite carte.

Une carte prépayée virtuelle permet à son porteur de recevoir un service de la part d'un fournisseur de service, le service étant payé par avance lors de l'achat de la carte. Pour cela, le porteur communique le code confidentiel de la carte à l'opérateur de la carte qui, après authentification du code, délivre le service demandé, en dépendance du crédit autorisé associé à la carte, et débite d'autant ce crédit.

On doit distinguer la carte prépayée virtuelle de la carte prépayée non virtuelle. Pour une carte prépayée virtuelle, toutes les caractéristiques de la carte, en particulier son crédit, sont gérées par un serveur centralisé. Pour une carte prépayée non virtuelle, la carte elle-même contient un circuit intégré avec microcontrôleur qui contient toutes les caractéristiques de la carte, y compris le crédit restant.

L'invention ne concerne que les cartes prépayées virtuelles, dites également "jetons virtuels".

A la différence des cartes prépayées non virtuelles, qui comprennent nécessairement un moyen électronique constitué par le circuit intégré, les cartes prépayées virtuelles peuvent être de deux sortes :

- les cartes prépayées virtuelles "immatérielles", qui sont constituées d'un code

confidentiel, tel qu'un simple numéro, qui est par exemple lisible sur la carte après grattage ;

- les cartes prépayées virtuelles "matérielles", qui sont constituées d'un dispositif physique, par exemple au moins une mémoire dans laquelle le code confidentiel a été pré-enregistré et qui généralement génère un code à chaque session d'utilisation de la carte.

Un utilisateur achète auprès d'un distributeur-commerçant une carte prépayée virtuelle. Elle est initialement créditée avant sa mise en service, d'un certain nombre d'unités, correspondant à son prix d'achat. Une unité permet de payer une part indivisible d'un service. Ce peut être de manière générale une unité monétaire ou une taxe de base, dans le cas d'une prestation téléphonique, ou une minute de communication, ou bien toute autre fraction d'un service.

La gestion de la carte prépayée virtuelle est réalisée par un serveur d'opérateur de cartes dont le rôle est de tenir à jour le crédit en unités de la carte ainsi que certaines données complémentaires telles que dates de validité, mise en opposition, etc.

Pour obtenir un service de la part du fournisseur de service, l'utilisateur doit d'abord prouver qu'il est en possession d'une carte prépayée virtuelle. Pour cela, le serveur d'opérateur de cartes authentifie la carte.

Si l'authentification de la carte prépayée virtuelle est réussie, le serveur d'opérateur indique au fournisseur de service le crédit restant sur la carte de l'utilisateur. Le fournisseur de service peut alors, en s'adressant au serveur d'opérateur,

débiter le compte de l'utilisateur en fonction du service rendu. Ce débit peut être réalisé soit avant la fourniture du service, soit au fur et à mesure de la fourniture du service, soit une fois le service rendu, soit par une combinaison de ces divers procédés.

Il est de l'intérêt commun de nombreux fournisseurs de service et opérateurs de cartes de passer des accords de reconnaissance mutuelle. Par conséquent, un fournisseur de service, en acceptant d'être payé par les cartes prépayées de différents opérateurs de cartes, multipliera les moyens de paiement offerts à ses clients et accroîtra son potentiel de vente. De même, un opérateur de cartes, en honorant les achats auprès de multiples fournisseurs de service, accroîtra le potentiel d'achat de ses cartes, et donc l'intérêt des clients pour ses cartes.

L'état de la technique a ainsi pour principal inconvénient que les fournisseurs de services doivent multiplier les interfaces logicielles de paiement correspondant aux différents opérateurs de cartes. Par ailleurs les opérateurs doivent se différencier sur les aspects visuels des cartes, afin que l'utilisateur de la carte puisse sélectionner correctement son moyen de paiement, par exemple sur un site internet, au moment de l'achat d'un service offert par un fournisseur de service.

L'invention a pour **objectif** de transférer automatiquement des codes confidentiels respectivement associés à des cartes prépayées depuis des terminaux d'utilisateur vers des serveurs d'opérateurs de cartes via une plateforme de

médiation afin que des fournisseurs de service n'aient recours qu'à une unique interface logicielle de paiement pour les cartes prépayées.

Pour atteindre cet objectif, un procédé pour transférer des codes confidentiels respectivement associés à des cartes prépayées depuis des terminaux vers des serveurs d'opérateur, les codes confidentiels résultant de l'application de numéros de série à des algorithmes d'embrouillement respectivement implémentés dans les serveurs, est caractérisé en ce qu'il comprend les étapes suivantes dans une plateforme :

avant l'utilisation des cartes, répartir des numéros de série respectivement associés à des cartes prépayées dans des tables de correspondance, et associer des adresses de serveurs d'opérateurs respectivement aux tables, lesdits algorithmes d'embrouillement étant identiques à un algorithme d'embrouillement commun, et

lors de l'utilisation d'une carte, appliquer un code confidentiel transmis depuis le terminal à un algorithme de débrouillement inverse dudit algorithme d'embrouillement commun pour déduire le numéro de série, rechercher la table de correspondance incluant le numéro de série déduit afin d'y lire l'adresse de serveur d'opérateur, et transmettre le code confidentiel au serveur d'opérateur désigné par ladite adresse.

La génération des numéros de série respectivement associés à des cartes prépayées est centralisée dans la plateforme afin que ceux-ci soient ordonnés, répartis et attribués entre différents opérateurs de cartes selon des tables de correspondance. Lorsqu'un code confidentiel associé à

une carte prépayée est reçu par la plateforme, celle-ci retrouve rapidement l'opérateur de ladite carte grâce à la table de correspondance comprenant le numéro de série déduit du code reçu.

Selon une autre caractéristique de l'invention, un serveur de fournisseur de service, auquel le terminal est initialement connecté, autorise une connexion de préférence sécurisée avec la plateforme afin que le terminal transmette le code confidentiel à la plateforme.

Le fournisseur de service peut rediriger tout utilisateur vers la plateforme, n'utilisant ainsi qu'une seule interface logicielle de paiement correspondant à la plateforme et non plus différentes interfaces logicielles correspondant à différents opérateurs de cartes.

En outre, l'utilisateur n'a plus besoin de retrouver l'opérateur de sa carte prépayée mais doit simplement composer le code confidentiel de sa carte.

L'invention concerne également une plateforme pour transférer des codes confidentiels respectivement associés à des cartes prépayées depuis des terminaux vers des serveurs d'opérateur, les codes confidentiels résultant de l'application de numéros de série à des algorithmes d'embrouillement respectivement implémentés dans les serveurs. La plateforme est caractérisée en ce qu'elle comprend :

un moyen pour répartir des numéros de série respectivement associés à des cartes prépayées dans des tables de correspondance,

un moyen pour associer des adresses de serveurs d'opérateurs respectivement aux tables,

un moyen pour appliquer un code confidentiel transmis depuis le terminal à un algorithme de débrouillement inverse d'un algorithme d'embrouillement commun qui est identique auxdits algorithmes d'embrouillement, pour déduire le numéro de série,

un moyen pour rechercher la table de correspondance incluant le numéro de série déduit et y lire l'adresse de serveur d'opérateur, et

un moyen pour transmettre le code confidentiel au serveur d'opérateur désigné par ladite adresse.

Enfin, l'invention se rapporte à un programme d'ordinateur apte à être mis en œuvre dans une plateforme pour transférer des codes confidentiels respectivement associés à des cartes prépayées depuis des terminaux vers des serveurs d'opérateurs, les codes confidentiels résultant de l'application de numéros de série à des algorithmes d'embrouillement respectivement implémentés dans les serveurs, ledit programme comprenant des instructions qui, lorsque le programme est chargé et exécuté sur ladite plateforme, réalisent les étapes selon le procédé de l'invention.

D'autres caractéristiques et avantages de la présente invention apparaîtront plus clairement à la lecture de la description suivante de plusieurs réalisations préférées de l'invention, données à titre d'exemples non limitatifs, en référence aux dessins annexés correspondants dans lesquels :

- la figure 1 est un bloc-diagramme schématique d'un système de télécommunications pour transférer des codes confidentiels depuis des terminaux

d'utilisateur vers des serveurs d'opérateur de cartes via une plateforme de médiation selon l'invention ;

- la figure 2 est un algorithme d'un procédé pour transférer un code confidentiel depuis un terminal d'utilisateur vers un serveur d'opérateur de cartes via la plateforme de médiation selon l'invention.

En référence à la figure 1, le **système de télécommunications** selon l'invention comprend au moins un terminal d'utilisateur tel qu'un terminal d'utilisateur T1, T2 ou T3, une plateforme de médiation PM, une base de données de médiation BDM en relation avec la plateforme de médiation PM, au moins un serveur d'opérateurs de cartes SOC éventuellement en relation avec une base de données d'opérateur BDO et au moins un serveur de fournisseur de service SFS.

La plateforme de médiation PM et les serveurs SOC et SFS communiquent entre eux de façon sécurisée à travers un réseau de télécommunications RT du type internet. Dans une variante, les serveurs communiquent entre eux par des lignes spécialisées ; en particulier les serveurs SOC et SFS et la plateforme PM sont en général respectivement localisés dans des sites géographiquement éloignés les uns des autres.

Les terminaux T1, T2 et T3 communiquent avec les serveurs SOC et SFS et avec la plateforme PM à travers des réseaux d'accès respectifs RA. Selon la réalisation illustrée à la figure 1, les terminaux sont reliés à des réseaux d'accès respectifs RA par des liaisons respectives LT1, LT2, LT3.

Un terminal d'utilisateur T1 est par exemple un terminal de radiocommunications cellulaire mobile, la

liaison LT1 est un canal de radiocommunications, et le réseau d'accès respectif RA comprend le réseau fixe d'un réseau de radiocommunications, par exemple de type GSM (Global System for Mobile communications) avec un service GPRS (General Packet Radio Service), ou de type UMTS (Universal Mobile Telecommunications System).

Selon un autre exemple, un terminal d'utilisateur T2 est un ordinateur personnel relié directement par modem à la liaison LT2 de type xDSL (Digital Subscriber Line) ou RNIS (Réseau Numérique à Intégration de Services) reliée au réseau d'accès RA correspondant.

Selon encore un autre exemple, un terminal d'utilisateur T3 comprend un dispositif ou objet électronique de télécommunications qui est personnel à l'utilisateur et qui peut être un assistant numérique personnel communicant PDA, ou un téléphone intelligent (SmartPhone). Plus généralement, le terminal T1, T2, T3 peut être tout autre terminal domestique communicant portable ou non tel qu'une console de jeux vidéo, ou un récepteur de télévision intelligent coopérant avec une télécommande à afficheur, ou un clavier alphanumérique servant également de souris à travers une liaison infrarouge.

Les terminaux d'utilisateur T1, T2 et T3 et les réseaux d'accès RA ne sont pas limités aux exemples ci-dessus et peuvent être constitués par d'autres terminaux et réseaux d'accès connus. Les terminaux d'utilisateur sont désignés indifféremment par T dans la suite de la description.

La **plateforme de médiation** PM comprend notamment une unité de traitement centrale UC, un générateur de

numéros de série GNS, un module de codage MC et un module d'interface logicielle de paiement IP.

La base de données de médiation BDM est liée à la plateforme de médiation PM, c'est-à-dire elle est soit intégrée dans la plateforme de médiation PM, soit incorporée dans un serveur de gestion de base de données et reliée à la plateforme de médiation par une liaison locale ou distante. La base de données BDM comprend notamment des informations sur des transactions effectuées entre des fournisseurs de service et des opérateurs de cartes et des informations nécessaires à la réalisation de l'invention telles que des tables de correspondance TC comprenant des numéros de série NS et associées à des identificateurs d'opérateur de cartes IOC.

Le générateur de numéros de série GNS génère des numéros de série NS qui sont constitués de préférence d'un même nombre de symboles alphanumériques, attribués et fournis à des opérateurs de cartes.

Le module de codage MC exécute des algorithmes prédéfinis, tels qu'un algorithme d'embrouillement AE, un algorithme de débrouillement AD, éventuellement un algorithme d'assemblage AG et un algorithme de désassemblage DG. Comme on le verra dans la suite, l'algorithme d'embrouillement sert à générer un code confidentiel en fonction d'un numéro de série et d'un certificat cryptographique, et l'algorithme d'assemblage sert dans une variante à générer un code confidentiel en fonction d'un code intermédiaire et d'une unité de redondance.

Le module d'interface logicielle de paiement IP active une interface logicielle de paiement d'un serveur de fournisseur de service SFS afin d'autoriser une connexion sécurisée avec un terminal d'utilisateur.

La plateforme PM comprend en outre des applications logicielles pour établir des connexions sécurisées avec des serveurs d'opérateur de cartes SOC.

Les **serveurs d'opérateurs de cartes** sont gérés respectivement par des opérateurs de cartes distincts qui vendent des cartes prépayées contenant un code confidentiel CC. Afin de ne pas surcharger la figure 1, on a représenté seulement deux serveurs d'opérateurs de cartes qui sont désignés indifféremment par SOC. Chaque serveur SOC certifie le code confidentiel d'une carte prépayée et le crédit associé à la carte prépayée au moyen d'une fonction de certification cryptographique propre à l'opérateur du serveur SOC. Le serveur SOC comprend une application logicielle pour une connexion sécurisée avec la plateforme PM.

La base de données d'opérateur BDO est liée à un serveur d'opérateur de cartes SOC, c'est-à-dire elle est soit intégrée dans le serveur d'opérateur de cartes SOC, soit incorporée dans un serveur de gestion de base de données et reliée au serveur d'opérateur de cartes SOC par une liaison locale ou distante. La base de données BDO comprend notamment une liste de numéros de série NS attribués et fournis à l'opérateur de cartes par la plateforme de médiation PM et une liste de certificats cryptographiques CERT.

Les **serveurs de fournisseurs de service** sont gérés respectivement par des fournisseurs de service proposant des services tels que la vente d'articles à "contenu numérique" sur un site internet, et passant des accords de reconnaissance mutuelle avec au moins

un opérateur de cartes afin d'utiliser des cartes prépayées comme moyen de paiement pour des transactions effectuées entre les deux parties. Afin de ne pas surcharger la figure 1, on a représenté seulement deux serveurs de fournisseurs de service qui sont désignés indifféremment par SFS. Chaque serveur SFS comprend une interface logicielle de paiement nécessaire à la connexion sécurisée entre la plateforme de médiation PM et un terminal d'utilisateur T.

La **carte prépayée** est une carte prépayée virtuelle "immatérielle", comportant simplement un code confidentiel CC seulement nécessaire, à l'exclusion de tout autre code, pour chaque accès à un service, la carte ne comportant aucun circuit intégré et étant appelée dans la suite "carte prépayée". Par exemple, le code CC est lisible sur un support cartonné ou plastique destiné à la vente, après grattage d'une zone prédéterminée. Le code CC peut être imprimé sur une facturette au moment de l'achat de la carte ou communiqué via un réseau de télécommunications contre un paiement supplémentaire du porteur de la carte.

Le **code confidentiel** CC d'une carte prépayée comprend généralement une dizaine de symboles alphanumériques et résulte de l'application d'un numéro de série NS et d'un certificat cryptographique CERT dérivé du numéro de série à l'algorithme d'embrouillement AE implémenté dans le serveur SOC de l'opérateur gérant la carte. Chaque code confidentiel est identifié et géré individuellement grâce au numéro de série qui lui est associé. La validité du code confidentiel est assurée par une fonction de

certification cryptographique. Il est alors impossible à des fraudeurs de deviner des codes dont les numéros de série seraient éventuellement proches de ceux qu'ils pourraient avoir à disposition.

Selon l'invention, l'algorithme d'embrouillement AE est commun à tous les opérateurs de cartes, c'est-à-dire que les algorithmes d'embrouillement implémentés dans les différents serveurs d'opérateurs de cartes SOC sont identiques à un algorithme d'embrouillement commun AE, afin que la plateforme de médiation PM puisse retrouver automatiquement un numéro de série NS en fonction d'un code confidentiel CC. La fonction de certification cryptographique est propre à chaque opérateur de cartes afin de garantir une stricte indépendance entre les différents opérateurs de cartes.

Par ailleurs, un opérateur de cartes peut réutiliser un numéro de série NS associé à une carte pour produire un nouveau code confidentiel lorsque la carte n'est plus valide, par exemple lorsque le crédit associé à la carte est épuisé ou lorsque la date de fin de validité de la carte a expiré. A cette fin, un numéro de version associé respectivement à un numéro de série NS est mis à jour afin de produire un nouveau certificat cryptographique CERT et par conséquent un nouveau code confidentiel CC associé à la carte qui est alors réutilisable.

L'invention s'applique à divers objets, qu'ils soient des services proprement dits ou qu'ils soient des produits obtenus indirectement par des services. Une réalisation préférée du procédé de transfert de l'invention est décrite ci-après pour transférer un code confidentiel CC associé à une carte prépayée depuis un terminal d'utilisateur T vers un serveur

d'opérateur de cartes SOC via la plateforme de médiation PM afin d'utiliser un service offert par un fournisseur de service et acquis au moyen de la carte prépayée. Il sera entendu que le procédé selon l'invention est aussi applicable pour transférer des codes confidentiels respectivement associés à des cartes prépayées depuis des terminaux vers des serveurs d'opérateurs.

En référence à la figure 2, le **procédé** pour transférer un code confidentiel associé à une carte prépayée depuis un terminal d'utilisateur vers un serveur d'opérateur de cartes via une plateforme de médiation selon l'invention comprend des étapes E1 à E7 lors de l'utilisation d'une carte, précédées d'étapes préliminaires E01 à E03 exécutées automatiquement dans la plateforme de médiation PM avant l'utilisation des cartes, par exemple en relation avec la fabrication des cartes.

A l'étape E01, le générateur de numéros de série GNS génère les numéros de série NS respectivement associés à des cartes prépayées. De préférence, chaque numéro de série comprend huit chiffres décimaux codés binaires ou sous forme hexadécimale. En variante, les numéros de série sont générés par un générateur chez le fabricant de cartes, remplaçant le générateur GNS, et enregistrés dans la base BDM de la plateforme de médiation PM.

A l'étape E02, l'unité centrale UC répartit les numéros de série dans des tables de correspondance TC. De préférence, chaque table TC comprend un nombre égal de numéros de série NS. Une division du nombre de numéros de série générés précédemment par le nombre de tables de correspondance envisagé révèle le nombre de numéros de série que comprend chaque table.

Dans un exemple pratique où les numéros de série comprennent huit chiffres, il est possible de former cent tables de correspondance désignées par les deux premiers "00" à "99" des huit chiffres, comprenant chacune un million de numéros de série ordonnés de manière croissante et pouvant être attribuées respectivement à cent opérateurs.

A l'étape E03, l'unité centrale UC associe des identificateurs d'opérateur de cartes IOC respectivement aux tables de correspondance TC, chaque identificateur IOC localisant l'adresse d'un serveur d'opérateur de cartes SOC. En variante, l'identificateur de serveur d'opérateur IOC est confondu avec l'adresse du serveur d'opérateur de cartes. Les tables de correspondance TC comprenant les numéros de série NS ainsi que les identificateurs IOC sont mémorisées dans la base de données de médiation BDM. Selon l'exemple pratique, les deux premiers chiffres des numéros de série de chaque table correspondent à un même nombre "00" à "99" qui désigne la table. Cependant plusieurs tables de correspondance désignées par un identificateur d'opérateur de cartes commun IOC peuvent être attribuées à un même opérateur de cartes. Par ailleurs, certaines tables peuvent être réservées pour un usage futur, c'est-à-dire qu'aucun identificateur d'opérateur de cartes IOC ne leur est attribué, pour prévoir d'éventuels partenariats avec de nouveaux opérateurs de cartes ou pour augmenter le nombre de numéros de série relatifs à des opérateurs de cartes déjà partenaires.

En variante, chaque table de correspondance TC comporte un unique numéro de série NS afin de réaliser une attribution secrète des identificateurs d'opérateur de cartes IOC. En effet, lorsque les deux

premiers chiffres des numéros de série indiquent un même nombre, l'identificateur d'opérateur de cartes IOC correspondant est rendu public aux opérateurs de cartes et chaque numéro de série est alors identifiable à l'opérateur de cartes auquel le numéro de série est rattaché. Dans cette variante, la confidentialité relative aux opérateurs de cartes est accrue au moyen d'un plus grand nombre de tables de correspondance mais au détriment d'une gestion plus complexe des tables.

Les numéros de série NS des tables de correspondance TC sont alors respectivement attribués aux opérateurs de cartes. Ensuite chaque opérateur de cartes génère chacun des codes confidentiels CC en appliquant l'un respectif des numéros de série qui lui sont attribués, et le certificat cryptographique qui est déterminé par application du numéro de série respectif à une fonction de certification qui est propre à l'opérateur de cartes, à l'algorithme d'embrouillement AE commun à tous les opérateurs de cartes. Chaque opérateur de cartes distribue et vend des cartes prépayées comprenant chacune l'un des codes confidentiels différents générés précédemment.

Initialement, un utilisateur retire chez un distributeur-commerçant, tel qu'une grande surface de distribution, une carte prépayée sous blister correspondant à un service donné, tel qu'un service de porte-monnaie électronique. Après avoir gratté une zone prédéterminée sur la carte prépayée pour y découvrir un code confidentiel CC, l'utilisateur peut utiliser la carte prépayée et consulte un site internet d'un fournisseur de service proposant des articles à vendre et acceptant la carte prépayée

comme moyen de paiement. Le terminal de l'utilisateur T est alors connecté au serveur de fournisseur de service SFS géré par le fournisseur de service.

A l'étape E1, l'utilisateur souhaitant acheter un article sur ledit site valide une sélection de l'article, et le terminal d'utilisateur T envoie une requête désignant l'article au serveur SFS. En réponse à la requête, le serveur SFS autorise une connexion sécurisée avec la plateforme de médiation PM afin que le terminal T et la plateforme PM puissent communiquer de façon sécurisée. Le serveur SFS n'établit donc plus de connexion directe avec un serveur d'opérateur de cartes SOC pour effectuer des transactions au moyen d'une interface appropriée mais se connecte à la plateforme PM et autorise une connexion sécurisée entre la plateforme PM et le terminal T au moyen de l'interface de paiement IP.

A l'étape E2, la plateforme PM invite l'utilisateur à composer le code confidentiel CC relatif à la carte prépayée qu'il a achetée précédemment, l'utilisateur n'ayant plus à sélectionner l'opérateur de la carte prépayée. Le terminal d'utilisateur T transmet alors une requête incluant le code confidentiel CC à la plateforme de médiation PM.

A l'étape E3, l'unité de traitement centrale UC reçoit la requête transmise par le terminal T et l'interprète, c'est-à-dire récupère le code confidentiel CC et le délivre au module de codage MC. Par ailleurs, le code confidentiel reçu CC est mémorisé dans la plateforme de médiation PM. Le module MC applique le code confidentiel CC à l'algorithme de débrouillement AD inverse dudit

algorithme d'embrouillement commun AE pour déduire et mémoriser le numéro de série NS.

A l'étape E4, l'unité centrale UC recherche la table de correspondance TC incluant le numéro de série déduit NS, par exemple en y extrayant les deux premiers chiffres.

Si la table de correspondance TC est trouvée, l'unité centrale UC y lit l'identificateur d'opérateur de cartes IOC, en l'occurrence l'adresse de serveur d'opérateur de cartes, à l'étape E5, c'est-à-dire l'unité centrale UC lit l'adresse de serveur d'opérateur dans la table de correspondance TC incluant le numéro de série NS déduit.

Si la table de correspondance TC n'est pas trouvée, le numéro de série n'est pas valide ou n'est attribué à aucun opérateur de carte connu de la plateforme PM, et la plateforme PM transmet un message d'erreur au terminal d'utilisateur T comme indiqué à une étape ER.

A l'étape E6, l'unité centrale UC transmet le code confidentiel CC, qui a été mémorisé temporairement à l'étape E3, au serveur d'opérateur de cartes SOC désigné par l'identificateur d'opérateur de cartes IOC lu, l'identificateur IOC indiquant l'adresse du serveur d'opérateur de cartes SOC auquel est rattaché le numéro de série déduit NS.

Par contre, le code confidentiel CC n'est pas transmis au serveur d'opérateur de cartes SOC lorsqu'une incohérence est détectée dans celui-ci ; par exemple, le numéro de série NS déduit du code confidentiel CC contient un symbole qui n'appartient pas à l'alphabet de symboles alphanumériques à partir duquel les numéros de série ont été générés initialement.

Le serveur SOC certifie le code confidentiel CC transmis par la plateforme au moyen de la fonction de certification cryptographique qui lui est propre. Le serveur SOC applique le code confidentiel CC à l'algorithme de débrouillement AD pour produire le numéro de série NS et un certificat cryptographique CERT. Le numéro de série déduit NS est appliqué à la fonction de certification cryptographique pour produire un autre certificat cryptographique. Si les certificats cryptographiques produits sont identiques, le numéro de série déduit NS est certifié. A la suite de cette certification, le serveur SOC retrouve alors les paramètres de la carte prépayée relative au code confidentiel CC, tel que le crédit associé à la carte.

A l'étape E7, après des échanges successifs avec le terminal T puis le serveur SFS aboutissant à la confirmation de la transaction, le serveur d'opérateur de cartes SOC transmet à la plateforme de médiation PM un message d'information MI relatif à la transaction effectuée entre le serveur d'opérateur de cartes SOC et le serveur de fournisseur de services SFS et correspondant à l'achat de l'article sélectionné par l'utilisateur. Grâce au message d'information MI, la plateforme PM garde en mémoire les traces des différentes transactions pour tenir à jour un état des reversements dus entre les opérateurs de cartes et les fournisseurs de service.

En variante, chaque code confidentiel CC résulte de l'application d'un code intermédiaire CI et d'une unité de redondance UR à un algorithme d'assemblage AG, comme décrit dans la demande de brevet EP 1 420 373 A1. Par exemple, le code intermédiaire CI, dit premier code intermédiaire, résulte de l'application

d'un numéro de série NS et d'un certificat cryptographique CERT dérivé du numéro de série à l'algorithme d'embrouillement AE, tandis que l'unité de redondance UR, dite première unité de redondance, résulte de l'application du premier code intermédiaire à un algorithme de redondance.

L'unité de redondance permet une détection rapide d'une erreur de saisie du code confidentiel et évite une certification inutile de ce dernier.

Dans cette variante, après l'étape E2, l'unité de redondance UR est contrôlée en fonction du code confidentiel CC par le module de codage MC à une étape E31. Par exemple, le code confidentiel CC est appliqué à un algorithme de désassemblage DG inverse de l'algorithme d'assemblage AG pour produire un deuxième code intermédiaire et une deuxième unité de redondance, et le deuxième code intermédiaire est appliqué à l'algorithme de redondance pour produire une troisième unité de redondance.

Si les deuxième et troisième unités de redondance sont identiques, le deuxième code intermédiaire est considéré comme valide et identique au code intermédiaire CI précédemment défini. Le module MC applique alors le deuxième code intermédiaire CI à l'algorithme de débrouillement AD inverse dudit algorithme d'embrouillement AE pour déduire le numéro de série NS à une étape E32. Le contrôle de l'unité de redondance est considéré comme réussi et autorise la transmission du code confidentiel CC au serveur d'opérateur de cartes SOC. Le procédé est ensuite poursuivi par l'étape E4 pour rechercher la table de correspondance TC incluant le numéro de série déduit NS.

Si les deuxième et troisième unités de redondance ne sont pas identiques, le code

confidentiel CC est considéré comme invalide et la plateforme PM transmet un message d'erreur au terminal d'utilisateur T comme indiqué à l'étape ER.

L'invention décrite ici concerne un procédé et une plateforme pour transférer des codes confidentiels respectivement associés à des cartes prépayées depuis des terminaux vers des serveurs d'opérateurs. Selon une implémentation préférée, les étapes du procédé de l'invention sont déterminées par les instructions d'un programme d'ordinateur incorporé dans une plateforme, telle que la plateforme de médiation PM. Le programme comporte des instructions de programme qui, lorsque ledit programme est chargé et exécuté dans la plateforme, dont le fonctionnement est alors commandé par l'exécution du programme, réalisent les étapes du procédé selon l'invention.

En conséquence, l'invention s'applique également à un programme d'ordinateur, notamment un programme d'ordinateur sur ou dans un support d'informations, adapté à mettre en œuvre l'invention. Ce programme peut utiliser n'importe quel langage de programmation, et être sous la forme de code source, code objet, ou de code intermédiaire entre code source et code objet tel que dans une forme partiellement compilée, ou dans n'importe quelle autre forme souhaitable pour implémenter le procédé selon l'invention.

Le support d'informations peut être n'importe quelle entité ou dispositif capable de stocker le programme. Par exemple, le support peut comporter un moyen de stockage ou support d'enregistrement, tel qu'une ROM, par exemple un CD ROM ou une ROM de circuit microélectronique, ou encore une clé USB, ou

un moyen d'enregistrement magnétique, par exemple une disquette (floppy disc) ou un disque dur.

D'autre part, le support d'informations peut être un support transmissible tel qu'un signal électrique ou optique, qui peut être acheminé via un câble électrique ou optique, par radio ou par d'autres moyens. Le programme selon l'invention peut être en particulier téléchargé sur un réseau de type internet.

Alternativement, le support d'informations peut être un circuit intégré dans lequel le programme est incorporé, le circuit étant adapté pour exécuter ou pour être utilisé dans l'exécution du procédé selon l'invention.

REVENDICATIONS

1 - Procédé pour transférer des codes confidentiels (CC) respectivement associés à des cartes prépayées depuis des terminaux (T) vers des serveurs d'opérateurs (SOC), les codes confidentiels résultant de l'application de numéros de série (NS) à des algorithmes d'embrouillement respectivement implémentés dans les serveurs (SOC), caractérisé en ce qu'il comprend les étapes suivantes dans une plateforme (PM) :

avant l'utilisation des cartes, répartir (E02) des numéros de série respectivement associés à des cartes prépayées dans des tables de correspondance (TC), et associer (E03) des adresses de serveurs d'opérateurs (SOC) respectivement aux tables (TC), lesdits algorithmes d'embrouillement étant identiques à un algorithme d'embrouillement commun (AE), et

lors de l'utilisation d'une carte, appliquer (E3) un code confidentiel (CC) transmis depuis le terminal (T) à un algorithme de débrouillement (AD) inverse dudit algorithme d'embrouillement commun (AE) pour déduire le numéro de série (NS), rechercher (E4) la table de correspondance (TC) incluant le numéro de série déduit afin d'y lire (E5) l'adresse de serveur d'opérateur, et transmettre (E6) le code confidentiel (CC) au serveur d'opérateur (SOC) désigné par ladite adresse.

2 - Procédé conforme à la revendication 1, selon lequel un serveur de fournisseur de service (SFS), auquel le terminal (T) est initialement connecté, autorise (E1) une connexion entre la plateforme (PM) et le terminal (T) afin que le terminal (T)

transmette (E2) le code confidentiel (CC) à la plateforme (PM).

3 - Procédé conforme à la revendication 1 ou 2, selon lequel la plateforme (PM) reçoit (E7), depuis le serveur d'opérateur (SOC), un message d'information (MI) relatif à une transaction effectuée entre le serveur d'opérateur (SOC) et le serveur de fournisseur de services (SFS).

4 - Procédé conforme à l'une quelconque des revendications 1 à 3, comprenant, en outre, lors de l'utilisation d'une carte, un contrôle (E31) d'une unité de redondance (UR) en fonction du code confidentiel (CC), et le code confidentiel (CC) est transmis au serveur d'opérateur (SOC) lorsque le contrôle est réussi (E32).

5 - Plateforme pour transférer des codes confidentiels (CC) respectivement associés à des cartes prépayées depuis des terminaux (T) vers des serveurs d'opérateur (SOC), les codes confidentiels résultant de l'application de numéros de série (NS) à des algorithmes d'embrouillement respectivement implémentés dans les serveurs (SOC), caractérisée en ce qu'elle comprend :

un moyen (UC) pour répartir des numéros de série respectivement associés à des cartes prépayées dans des tables de correspondance (TC),

un moyen (UC) pour associer des adresses de serveurs d'opérateurs (SOC) respectivement aux tables (TC),

un moyen (MC) pour appliquer un code confidentiel (CC) transmis depuis le terminal (T) à un algorithme de débrouillement (AD) inverse d'un

algorithme d'embrouillement commun (AE) qui est identique auxdits algorithmes d'embrouillement, pour déduire le numéro de série (NS),

un moyen (UC) pour rechercher la table de correspondance (TC) incluant le numéro de série déduit et y lire l'adresse de serveur d'opérateur, et

un moyen (UC) pour transmettre le code confidentiel (CC) au serveur d'opérateur (SOC) désigné par ladite adresse.

6 - Programme d'ordinateur apte à être mis en œuvre dans une plateforme (PM) pour transférer des codes confidentiels (CC) respectivement associés à des cartes prépayées depuis des terminaux (T) vers des serveurs d'opérateur (SOC), les codes confidentiels résultant de l'application de numéros de série (NS) à des algorithmes d'embrouillement respectivement implémentés dans les serveurs (SOC), ledit programme comprenant des instructions qui, lorsque le programme est chargé et exécuté dans ladite plateforme, réalisent les étapes de :

avant l'utilisation des cartes, répartir (E02) des numéros de série respectivement associés à des cartes prépayées dans des tables de correspondance (TC), et associer (E03) des adresses de serveurs d'opérateurs (SOC) respectivement aux tables (TC), lesdits algorithmes d'embrouillement étant identiques à un algorithme d'embrouillement commun (AE), et

lors de l'utilisation d'une carte, appliquer (E3) un code confidentiel (CC) transmis depuis le terminal (T) à un algorithme de débrouillement (AD) inverse dudit algorithme d'embrouillement commun (AE) pour déduire le numéro de série (NS), rechercher (E4) la table de correspondance (TC) incluant le numéro de série déduit afin d'y lire (E5) l'adresse de serveur

d'opérateur, et transmettre (E6) le code confidentiel (CC) au serveur d'opérateur (SOC) désigné par ladite adresse.

FIG. 1

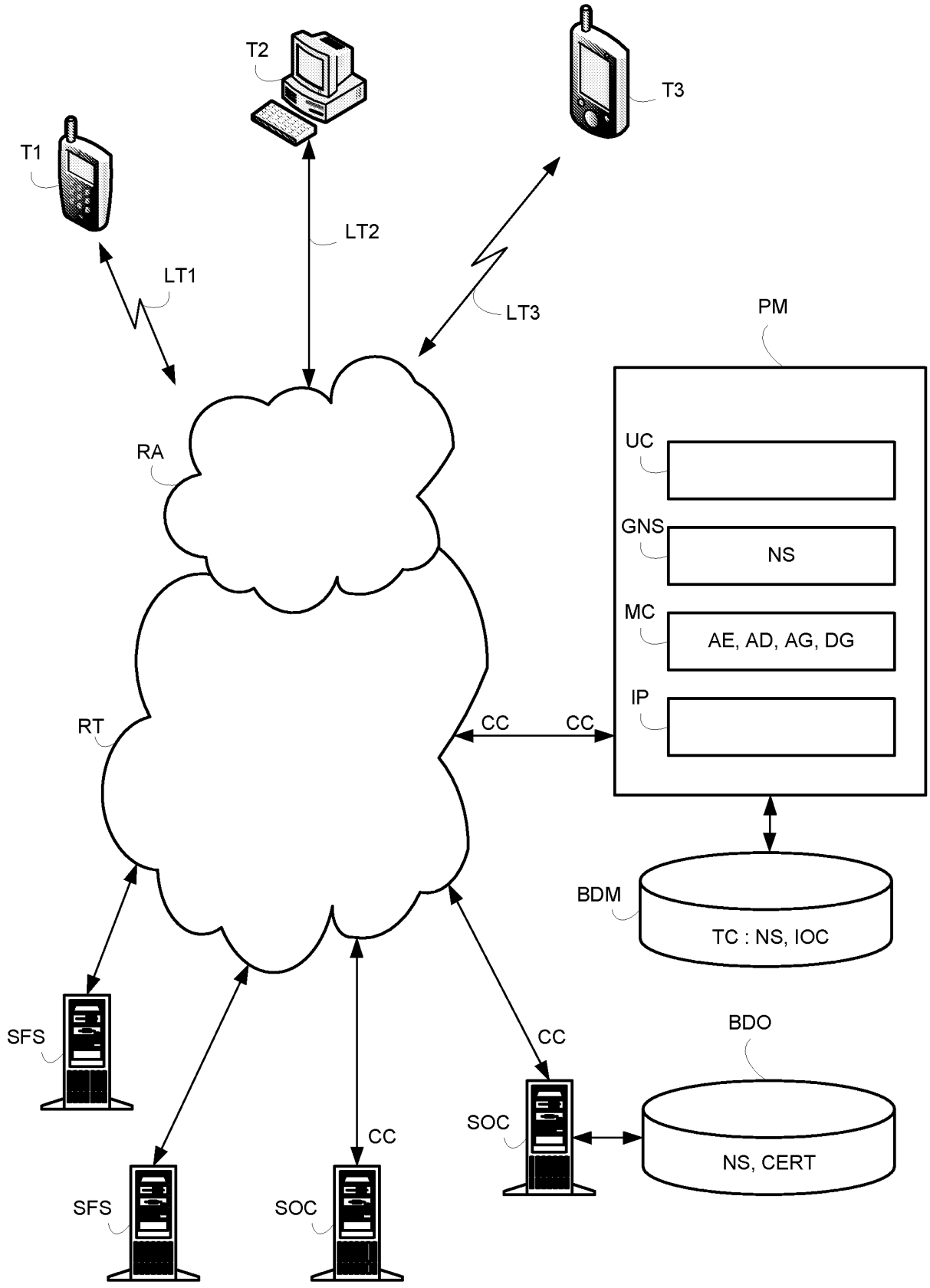
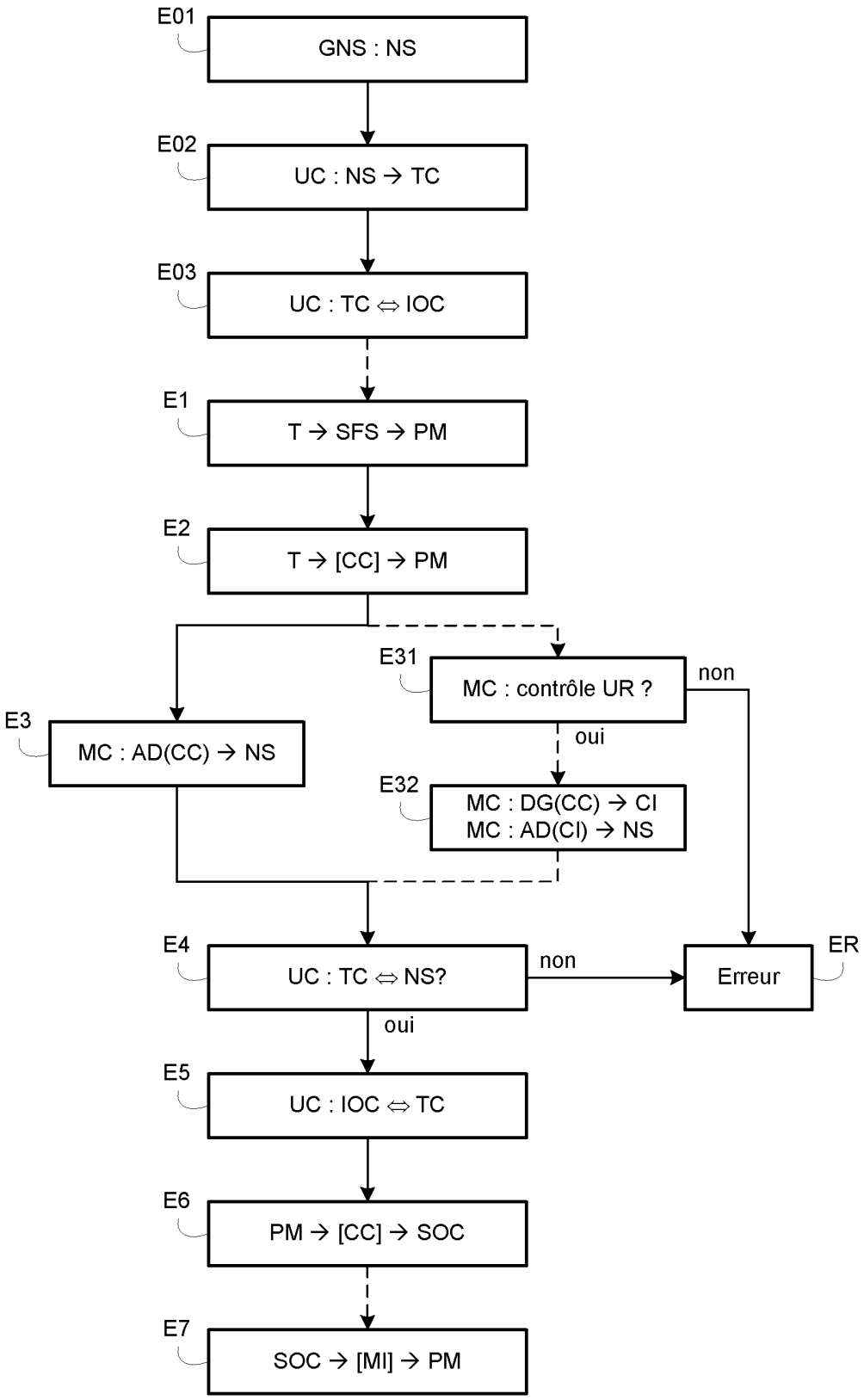

T1
T2
T3
LT1
LT2
LT3
RA
RT
PM
UC
GNS
NS
MC
AE, AD, AG, DG
IP
CC
CC
BDM
TC : NS, IOC
BDO
NS, CERT
SFS
SFS
SOC
SOC
CC
CC

FIG. 2


E01
GNS : NS
E02
UC : NS → TC
E03
UC : TC ⇔ IOC
E1
T → SFS → PM
E2
T → [CC] → PM
E31
MC : contrôle UR ?
non
oui
E3
MC : AD(CC) → NS
E32
MC : DG(CC) → CI
MC : AD(CI) → NS
E4
UC : TC ⇔ NS?
non
ER
Erreur
oui
E5
UC : IOC ⇔ TC
E6
PM → [CC] → SOC
E7
SOC → [MI] → PM