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

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
9 janvier 2003 (09.01.2003)

PCT

(10) Numéro de publication internationale
WO 03/003772 A2

(51) Classification internationale des brevets[7] : H04Q 7/32

(21) Numéro de la demande internationale :
PCT/FR02/02088

(22) Date de dépôt international : 17 juin 2002 (17.06.2002)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
01/07865 15 juin 2001 (15.06.2001) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **GEMPLUS** [FR/FR]; Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F-13420 Gemenos (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **HU, Hai-tao** [FR/CN]; Room B05, Heng Chuan Apartments, N° 168 Xi Ba He Road, Chao Yang District, Beijing 100028 (CN). **FAN, Li-Jun** [CN/CN]; 7-606 An Hui Dong Li, Chao Yang District, Beijing 100101 (CN). **ZHAO, Zai-Xing** [CN/CN]; N° 100 Ping Le Yuan, Chao Yang District, Beijing 100101 (CN).

(74) Mandataire : **AIVAZIAN, Denis**; c/o Gemplus, Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F-13420 Gemenos (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet 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 à l'identité de l'inventeur (règle 4.17.i)) pour les désignations suivantes AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI,*

*[Suite sur la page suivante]*

(54) Title: METHOD FOR REMOTE LOADING OF AN ENCRYPTION KEY IN A TELECOMMUNICATION NETWORK STATION

(54) Titre : PROCEDE DE CHARGEMENT A DISTANCE D'UNE CLE DE CRYPTAGE DANS UN POSTE D'UN RESEAU DE TELECOMMUNICATION

(57) Abstract: When a system detects that a transaction key in the SIM card (18) of a mobile station (36, 38) is non-existent or is no longer valid, the method automatically performs the following steps: generating in the application key server (42) a transaction key; encrypting the transaction key in the application server (42) using a transmission key generated when the SIM card was customized; transmitting the encrypted transition key via the SMS service centre (40) to the mobile station (36, 38); decrypting in the SIM card (18) the encrypted transaction key using the transmission key; and recording the decrypted transaction key in the SIM card storage. Furthermore, the method enables to select among several possible keys one key which corresponds both to a specific application and to a specific service provider.

(57) Abrégé : Dès qu'un système détecte qu'une clé de transaction dans la carte SIM (18) d'un poste mobile (36, 38) n'existe pas ou n'est plus appropriée, le procédé réalise automatiquement les étapes suivantes :- générer dans le serveur de clés d'application (42) une clé de transaction,- crypter la clé de transaction dans le serveur de l'application (42) à l'aide d'une clé de transmission créée lors de la personnalisation de la carte SIM, - transmettre la clé de transaction cryptée via le serveur centre SMS (40) au poste mobile (36, 38), - décrypter dans la carte SIM (18) la clé de transaction cryptée à l'aide de la clé de transmission, et - enregistrer la clé de transaction décryptée dans la mémoire de la carte SIM. En outre, le procédé permet de sélectionner parmi plusieurs clés possibles une clé qui correspond à la fois à une certaine application et à un certain fournisseur de services.

WO 03/003772 A2

*FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

- *relative au droit du déposant de demander et d'obtenir un brevet (règle 4.17.ii)) pour les désignations suivantes AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*
- *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour toutes les désignations*
- *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

**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.*

# PROCEDE DE CHARGEMENT A DISTANCE D'UNE CLE DE CRYPTAGE DANS UN POSTE D'UN RESEAU DE TELECOMMUNICATION

L'invention concerne les systèmes de télécommunication, par exemple de type GSM et, plus particulièrement dans de tels systèmes, un procédé pour charger des clés de cryptage dans les postes mobiles en vue de sécuriser les transactions effectuées à partir desdits postes mobiles. GSM est l'acronyme de l'expression anglo-saxonne "Global System for Mobile communications".

Un système de télécommunication du type GSM permet, en premier lieu, de connecter entre eux des abonnés pouvant appartenir à différents réseaux téléphoniques.

Il permet aussi de fournir aux abonnés d'autres services tels que de l'information, des opérations de banque et de bourse, etc ... .

A cet effet, chaque poste mobile est équipé d'une carte SIM (SIM étant l'acronyme pour l'expression anglo-saxonne "Subscriber Identity Module" ou Module d'identification d'abonné en français) qui est un circuit intégré prévu, notamment, pour mettre en oeuvre diverses applications telles que les services mentionnés ci-dessus.

Les informations nécessaires à la mise en oeuvre de ces applications sont chargées dans la carte SIM, en général au point de vente, sous forme de fichiers informatiques qui sont enregistrés dans les mémoires du circuit intégré.

Certaines des applications telles que celles relatives à la banque et à la bourse nécessitent que les transactions qui sont effectuées soient sécurisées. A cet effet, le transfert des informations entre le poste mobile et le fournisseur du service est crypté selon

des algorithmes employant des clés de cryptage, ces clés étant introduites dans la carte SIM au moment de la personnalisation de la carte SIM.

Cette manière de procéder présente, notamment, les inconvénients suivants :

- les clés introduites ne peuvent concerner que les applications qui sont chargées de sorte que pour une nouvelle application, il est nécessaire de fournir une nouvelle carte SIM avec les clés qui lui sont affectées,
- il n'est pas possible de changer ou mettre à jour les clés des applications au cours de la vie de la carte SIM, sauf à changer la carte au point de vente.

Un but de la présente invention est donc de mettre en oeuvre un procédé de chargement de carte SIM qui permet de charger à distance de manière sécurisée des clés de cryptage d'une ou plusieurs applications, ce qui évite le retour de la carte au point de vente ainsi que son retrait pour la remplacer par une autre avec d'autres clés.

Ce but est atteint en effectuant ce chargement des clés d'une ou plusieurs applications par l'intermédiaire de messages transmis au poste mobile sur un canal de communication des messages courts, tel que celui connu sous le sigle SMS, acronyme de l'expression anglo-saxonne "Short Message Service".

Pour assurer la sécurité de la transmission, ces messages transmis sont cryptés à l'aide d'une clé dite de "transport" ou de "transmission" qui est créée et enregistrée dans la carte SIM lors de sa personnalisation chez un opérateur.

Un autre but de la présente invention est de mettre en oeuvre un procédé de chargement à distance de manière

sécurisée de clés de cryptage dans une carte d'identification d'abonné dans lequel le chargement est précédé d'une étape de détection d'une absence de clé ou d'un besoin de mise à jour d'une clé dans la carte d'identification d'abonné.

L'invention concerne donc un procédé de chargement d'au moins une clé, notamment associée à une application de transaction dans une carte ou module d'identification d'abonné SIM pour poste mobile d'un réseau de télécommunication caractérisé en ce qu'il comprend l'étape suivante consistant à :

- charger au moins ladite clé au cours d'une session de télécommunication du poste mobile sur le réseau de télécommunication.

L'étape de chargement est précédée d'une étape consistant à détecter dans la carte d'identification d'abonné SIM l'absence de clé ou un besoin de mise à jour de ladite clé.

L'étape consistant à détecter l'absence de clé ou le besoin de mise à jour de ladite clé est effectuée par analyse d'au moins un message d'une session de télécommunication. Cette analyse est effectuée soit dans la carte d'identification d'abonné, soit dans un serveur de clés connecté au réseau de télécommunication.

L'analyse d'au moins un message d'une session de télécommunication est effectuée dans un serveur connecté au serveur de clés.

Le serveur connecté au serveur de clés est un serveur de l'application associée.

Le serveur connecté au serveur de clés est le serveur du fournisseur de services de l'application associée.

Le message qui est analysé est un certificat cryptographique.

Le message qui est analysé est une requête de la carte d'identification d'abonné SIM.

Les étapes pour télécharger de manière sécurisée au moins ladite clé cryptographique consistent à :

- crypter la clé cryptographique fournie par le serveur de clés à l'aide d'une clé de transmission,
- transmettre la clé cryptographique cryptée à la carte d'identification d'abonné SIM,
- décrypter dans la carte d'identification d'abonné SIM la clé cryptographique à l'aide de la clé de transmission, et
- enregistrer la clé cryptographique décryptée dans la carte d'identification d'abonné SIM.

L'étape consistant à télécharger ladite clé cryptographique est effectuée par un canal de transmission des messages courts du type connu sous l'acronyme "SMS" ou "ESMS.

L'invention concerne également une carte d'identification d'abonné SIM pour permettre la mise en oeuvre du procédé, caractérisée en ce qu'elle comprend un programme apte à détecter l'absence de clé ou le besoin de mise à jour de la clé.

La carte d'identification d'abonné SIM est caractérisée en ce qu'elle comprend, en outre, un programme apte à émettre un message de requête ou de mise à jour d'une clé cryptographique.

Le serveur de clés d'application pour mettre en oeuvre le procédé est caractérisé en ce qu'il comprend un programme apte à transmettre sur requête la clé cryptographique cryptée à une carte d'identification d'abonné SIM.

Le serveur du fournisseur de services pour mettre en oeuvre le procédé est caractérisé en ce qu'il comprend un programme apte à analyser un message d'une session de télécommunication pour déterminer l'absence de clé ou le besoin de mise à jour d'une clé cryptographique

Le serveur du fournisseur de services est caractérisé en ce que le programme détecte l'absence de clé ou le besoin de clé cryptographique à partir de la valeur d'un certificat cryptographique.

D'autre part, on note que la solution de l'invention permet une application dynamique pour les raisons suivantes :

- la mise à jour ou transmission de nouvelles clés est automatique ;
- l'invention propose une solution à un problème technique supplémentaire qui provient du fait qu'une même application peut être partagée par des fournisseurs de services différents, exigeant chacun des clés de transaction différentes pour utiliser l'application. L'invention permet de sélectionner la clé correspondant au fournisseur de services concerné par la transaction à effectuer : elle permet ainsi pour une même application de choisir parmi plusieurs clés possibles celles qui correspond à un certain fournisseur de service à un instant donné. Cette solution rend ainsi implicitement possible l'application dynamique de l'invention ;
- la solution est basée sur un technologie de communication distante et suffisamment rapide.

D'autres caractéristiques et avantages de la présente invention apparaîtront à la lecture de la description suivante d'un exemple particulier de réalisation,

ladite description étant faite en relation avec les dessins joints dans lesquels :

- la figure 1 est un schéma simplifié d'un poste mobile d'un réseau de télécommunication, par exemple de type GSM, et
- la figure 2 est un schéma d'un réseau de télécommunication, par exemple du type GSM, mettant en oeuvre le procédé de l'invention.

Comme le montre le schéma de la figure 1, un poste de téléphone mobile de type GSM comprend :

- un émetteur-récepteur 10 relié à une antenne 12 pour émettre et recevoir des signaux radioélectriques,
- un modulateur-démodulateur 14 pour moduler et démoduler les signaux radioélectriques,
- un microprocesseur 16 pour générer les signaux de modulation et interpréter les signaux démodulés de manière à réaliser les fonctions de télécommunication, et
- une carte ou module d'identification d'abonné SIM 18 pour personnaliser le poste mobile en fonction de l'abonné, notamment lui affecter un numéro d'appel, lui accorder des droits d'accès à certains services et pas à d'autres, lui permettre d'effectuer certaines transactions financières comme des virements bancaires, des achats/ventes en bourse, etc ... .

La carte SIM 18 est connectée au microprocesseur 16 par l'intermédiaire d'un dispositif à contacts 20.

S'agissant de transactions financières, il est important qu'elles soient effectuées avec un maximum de sécurité. Cette sécurité passe par un cryptage ou chiffrement des messages suivi d'un décryptage ou déchiffrement de ces messages cryptés. Ces

cryptages/décryptages sont réalisés à l'aide d'algorithmes bien connus utilisant des clés connus uniquement de l'opérateur ou gestionnaire de l'application et de l'utilisateur de l'application ou plus exactement connus de sa carte SIM.

Dans l'état actuel de l'art, la clé de transaction de la carte SIM de l'utilisateur est enregistrée au moment du chargement de l'application dans la carte SIM, ce qui n'est pas propice pour effectuer un changement de clé qui peut être rendu nécessaire pour des raisons de sécurité.

L'invention propose de réaliser ce changement de clé ou, initialement, le chargement d'une clé pour une nouvelle application, en utilisant un canal de communication des messages courts plus connu sous l'acronyme SMS pour l'expression anglo-saxonne "Short Message Service". Ce chargement ou changement est initié soit par l'utilisateur, soit par le fournisseur de services de l'application, par exemple une banque pour des opérations bancaires.

Le schéma de la figure 2 montre les intervenants dans le procédé de l'invention. Les abonnés 30 et 32 à un réseau de télécommunication 34, par exemple du type GSM, sont équipés respectivement chacun d'un poste mobile 36 et 38. Chaque poste mobile 36, 38 est muni d'une carte ou module d'identification d'abonné SIM, comme celle référencée 18 sur la figure 1, qui a été personnalisée pour mettre en oeuvre au moins une application nécessitant une sécurité des transactions effectuées grâce à l'application, par exemple des transactions bancaires ou boursières avec une banque.

Le réseau GSM 34 est sous le contrôle d'un opérateur de télécommunication (non représenté) et ce réseau est

connecté à un centre SMS 40. C'est ce centre SMS 40 qui est connecté à un serveur de clés d'application 42. Le centre SMS 40 génère des messages dits "SMS" qui ont un format déterminé. Il peut aussi générer des messages "enrichis" appelés "ESMS" qui peuvent véhiculer des instructions de type informatique.

Le serveur de clés d'application 42 est connecté à un module de sécurité 44 connu sous l'acronyme "HSAM" pour l'expression anglo-saxonne "Host Secure Access Module", ce module 44 pouvant être connecté à une carte à puce électronique 46.

Le chargement ou le changement de clé est initié soit par la carte SIM du poste mobile, soit par le serveur de clés d'application, après détection d'une absence de clé ou d'un besoin de mise à jour de la clé par analyse d'un message d'une session de télécommunication.

Dans le cas où l'initiateur du chargement ou du changement de la clé est la carte SIM, les opérations ou étapes sont les suivantes :

(a) générer dans la carte SIM 18 du poste mobile 30, 32 un message de requête de chargement d'une clé de cryptage pour les transactions selon l'application,

(b) crypter le message de requête dans la carte SIM en utilisant une clé de transmission enregistrée lors de la personnalisation de la carte SIM,

(c) transmettre le message de requête crypté au serveur de clés d'application 42, via le serveur SMS 40,

(d) décrypter dans le serveur de l'application 42 le message de requête crypté à l'aide de la clé de transmission,

(e) générer dans le serveur de clés d'application 42, une clé de transaction en utilisant le module HSAM 44, et, éventuellement, la carte à puce électronique 46,

(f) crypter la clé de transaction dans le serveur de clés d'application 42 à l'aide de la clé de transmission,

(g) transmettre la clé de transaction cryptée via le centre SMS 40 au poste mobile 36 ou 38,

(h) décrypter dans la carte SIM 18 la clé de transaction cryptée à l'aide de la clé de transmission,

(i) enregistrer la clé de transaction décryptée dans la mémoire de la carte SIM.

Dans le cas où le chargement ou changement de la clé de transaction est initié par le serveur de clés d'application 42, les étapes sont les suivantes :

- détecter dans le serveur de clés d'application 42 que dans un message de transaction en provenance du poste mobile 36, 38 la clé de transaction n'existe pas ou n'est plus appropriée pour effectuer la transaction,

les autres étapes sont identiques aux étapes (e) à (i) de la première variante, soit,

(e) générer dans le serveur de l'application 42 une clé de transaction en utilisant le module HSAM 44, et éventuellement la carte à puce 46,

(f) crypter la clé de transaction dans le serveur de l'application 42 à l'aide de la clé de transmission,

(g) transmettre la clé de transaction cryptée via le serveur SMS 40 au poste mobile,

(h) décrypter dans la carte SIM la clé de transaction cryptée à l'aide de la clé de transmission, et

(i) enregistrer la clé de transaction décryptée dans la mémoire de la carte SIM.

Dans le cas d'une application de type bancaire qui est utilisée par plusieurs banques, chaque banque sera équipée d'un serveur de clés d'application 42, d'un module HSAM 44 et d'une carte à puce électronique 46.

L'application bancaire est chargée dans la carte SIM au point de vente, ce dernier étant en liaison avec le serveur d'application 42.

Une première clé de transaction peut être enregistrée dans la carte SIM au point de vente. Dans le cas où la clé de transaction n'est pas chargée lors du chargement de l'application, elle le sera avant toute transaction soit à l'initiative du poste mobile ou celle du serveur de clés d'application 42, lors de la réception de la première transaction de l'application.

Le contenu de la clé de transaction dépend du serveur de clés d'application concerné et de la banque qui est concernée par la transaction. Comme un utilisateur peut être mis en relation avec plusieurs banques pour la même application, chaque banque a sa propre clé de transaction qui doit être enregistrée dans la carte SIM. Pour sélectionner la bonne clé de transaction, celle qui est affectée à la banque avec laquelle la transaction est effectuée, le message SMS crypté est précédé d'octets indiquant en clair, c'est-à-dire, sans cryptage, l'identité de la banque.

Comme indiqué ci-dessus, la mise à jour ou le chargement d'une clé de transaction est provoquée soit par la carte SIM 18, soit par le serveur de clés d'application 42.

Dans le premier cas, s'il n'y a pas de clé ou une mauvaise clé dans la carte SIM lors d'une transaction

reçue et codée en message court SMS, l'application dans la carte SIM retourne automatiquement au serveur de clés d'application 42 un message court SMS pour demander la mise en oeuvre de la procédure de mise à jour ou de chargement de la clé. L'application dans la carte SIM est capable de déterminer si la clé en sa possession est bonne (ou existe) en analysant le message d'une session de communication.

Dans le deuxième cas, le serveur de clés d'application est capable de déterminer si la clé de transaction enregistrée dans la carte SIM est bonne ou mauvaise en analysant le message d'une session de communication. Si la clé est mauvaise, le serveur de clés d'application envoie un message court SMS à la carte en question, la carte étant identifiée par son numéro de série et celui du mobile.

Le procédé selon l'invention a été décrit en prévoyant une détection automatique d'une absence de clé ou d'un besoin de mise à jour de clé soit par la carte SIM, soit par le serveur de clés d'application. Cependant, le procédé peut être mis en oeuvre sans faire appel à une telle détection automatique mais à la suite d'une initiative volontaire de l'utilisateur du poste mobile ou du fournisseur de services.

La détection automatique de l'absence de clé ou du besoin de mise à jour de la clé est effectuée par un programme approprié qui, selon le cas, est chargé dans la carte SIM ou dans le serveur de clés d'application.

Dans le cas d'un chargement ou changement à la suite d'une initiative volontaire, le programme de l'application présentera une option à cet effet.

L'analyse du message d'une session de télécommunication pour déterminer l'absence de clé ou le besoin de mise à

jour d'une clé peut, au lieu d'être réalisée par le serveur de clés d'application 42, être effectuée par un serveur connecté au serveur de clés d'application tel qu'un serveur de l'application associée ou un serveur du fournisseur de services de l'application associée.

Le message qui est analysé est un certificat cryptographique ou une requête de la carte d'identification d'abonné SIM 18.

La carte d'identification d'abonné 18 comprend un programme apte à détecter l'absence de clé ou le besoin de mise à jour de la clé. En outre, elle est apte à émettre un message de requête ou de mise à jour de la clé de transaction.

Le serveur de clés d'application comprend un programme qui est apte à transmettre sur requête la clé de transaction à la carte d'identification d'abonné.

Dans une variante, le serveur du fournisseur de service comprend un programme apte à analyser un message d'une session de communication pour détecter l'absence de clé ou le besoin de mise à jour de clé cryptographique.

# R E V E N D I C A T I O N S

1. Procédé de chargement d'au moins une clé cryptographique, notamment associée à une application de transaction, dans une carte ou module d'identification d'abonné SIM (18) pour poste mobile (36, 38) d'un réseau de télécommunication au cours d'une session de télécommunication sécurisée du poste mobile,
caractérisé en ce qu'il comprend l'étape consistant à :
- détecter automatiquement une absence de clé ou un besoin de mise à jour d'une clé dans la carte SIM (18).

2. Procédé selon la revendication 1, caractérisé en ce que l'étape consistant à détecter dans la carte d'identification d'abonné SIM (18) une absence de clé ou un besoin de mise à jour de ladite clé est effectuée par une analyse d'au moins un message d'une session de télécommunication.

3. Procédé selon la revendication 2, caractérisé en ce que ladite analyse d'au moins un message d'une session de télécommunication est effectuée dans la carte d'identification d'abonné SIM (18).

4. Procédé selon la revendication 2, caractérisé en ce que ladite analyse d'au moins un message d'une session de télécommunication est effectuée dans le serveur de clés.

5. Procédé selon la revendication 2, caractérisé en ce que ladite analyse d'au moins un message d'une session

de télécommunication est effectuée dans un serveur connecté au serveur de clés.

6. Procédé selon l'une des revendications 2 à 5, caractérisé en ce que le message qui est analysé est un certificat cryptographique.

7. Procédé selon l'une des revendications 2 à 5, caractérisé en ce que le message qui est analysé est une requête de la carte d'identification d'abonné SIM (18).

8. Procédé selon l'une quelconque des revendications 1 à 7, caractérisé en ce que l'étape consistant à télécharger ladite clé cryptographique est effectuée par un canal de transmission des messages courts du type connu sous l'acronyme "SMS" ou "ESMS.

9. Procédé selon la revendication 8, caractérisé en ce que le message court comprend une identité d'un fournisseur de service correspondant à l'application de transaction concernée afin de sélectionner la bonne clé concernée par la transaction effectuée.

10. Procédé selon la revendication 9, caractérisé en ce que le message court comporte en clair l'identité du fournisseur du service et la clé cryptographique cryptée.

11. Carte d'identification d'abonné SIM (18) pour permettre la mise en oeuvre du procédé selon la revendication 3, caractérisée en ce qu'elle comprend un

programme apte à détecter l'absence de clé ou le besoin de mise à jour de la clé.

12. Carte d'identification d'abonné SIM (18) selon la revendication 11, caractérisée en ce qu'elle comprend, en outre, un programme apte à émettre automatiquement un message de requête ou de mise à jour d'une clé cryptographique.

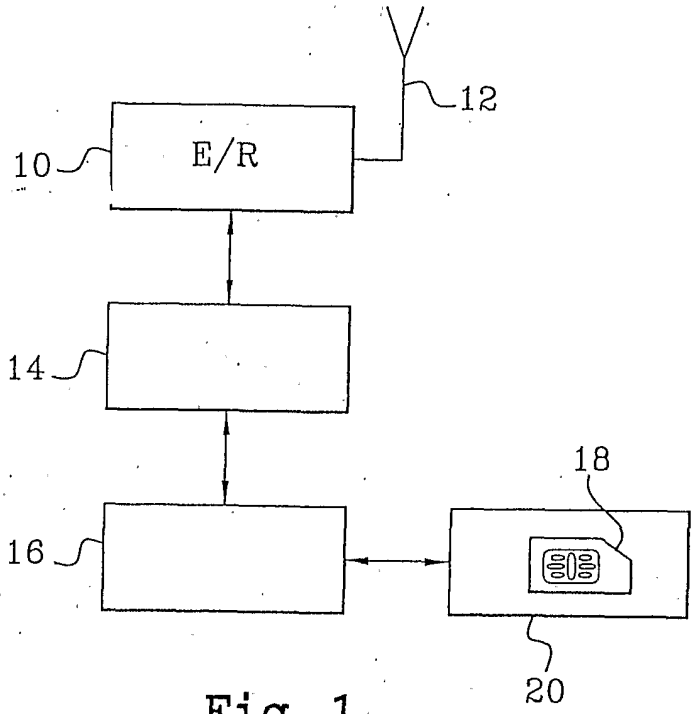


Fig. 1

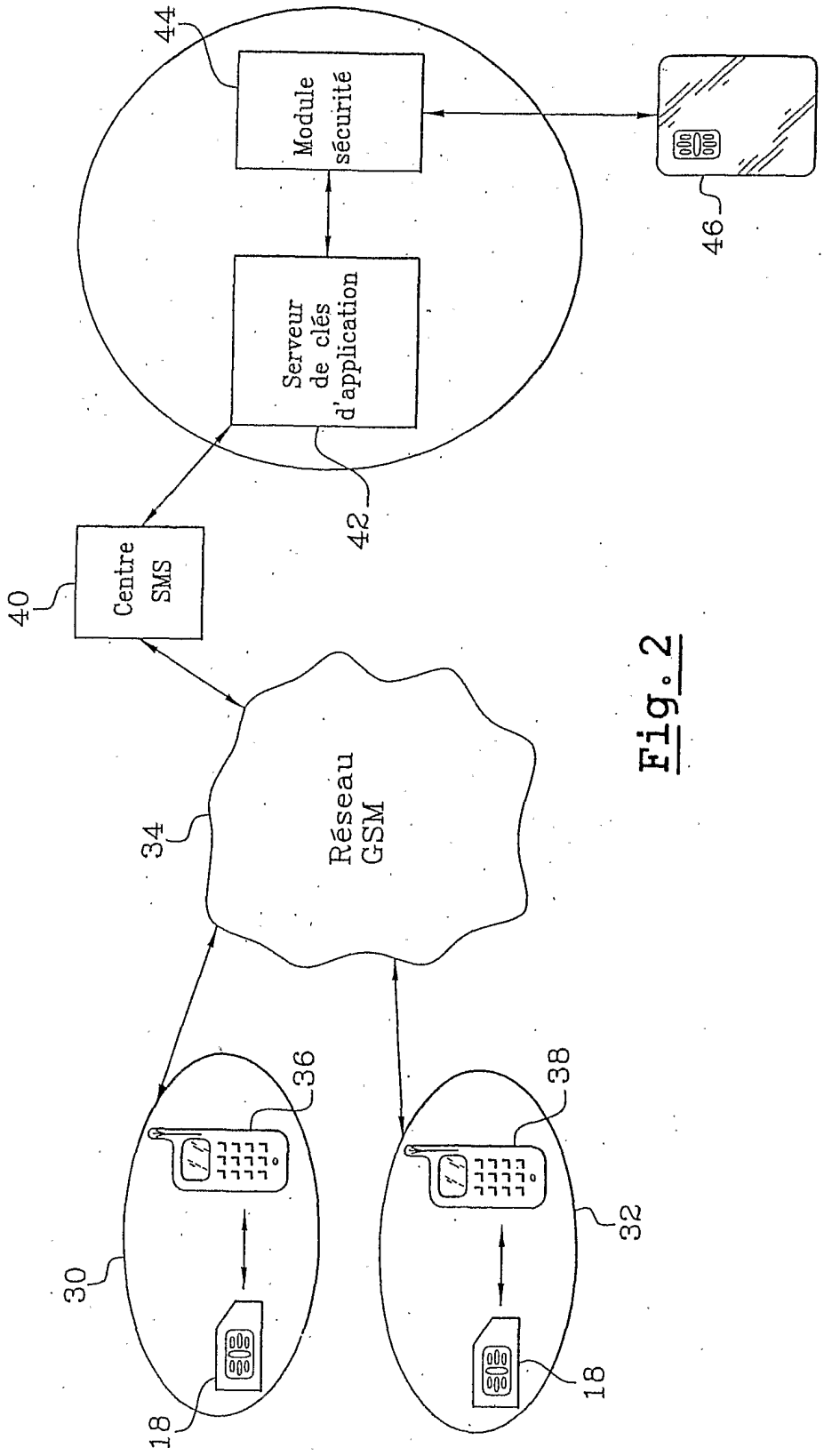
44
Module sécurité
Serveur de clés d'application
42
46
40
Centre SMS
34
Réseau GSM
36
38
30
32
18
18

Fig. 2