(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 763 773**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **97 06428**

(51) Int Cl^6 : **H 04 M 3/38,** H 04 Q 7/32

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 20.05.97.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 27.11.98 Bulletin 98/48.

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

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

(71) **Demandeur(s) :** *GEMPLUS SOCIETE EN COMMANDITE PAR ACTIONS* — FR.

(72) **Inventeur(s) :** CARRARA JEAN LOUIS.

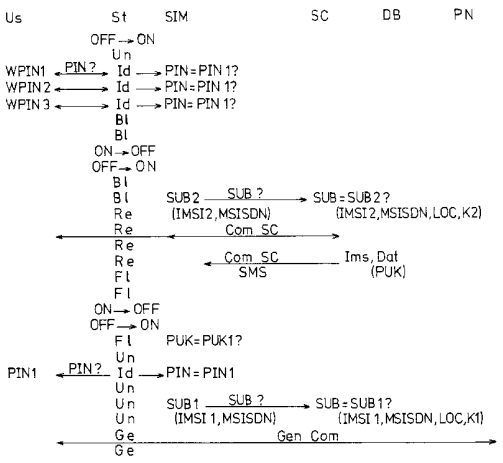
(73) **Titulaire(s) :**

(74) **Mandataire(s) :** CABINET BALLOT SCHMIT.

(54) DEBLOCAGE A DISTANCE D'ACCES A UN SERVICE DE TELECOMMUNICATION.

(57) L'invention concerne le déblocage d'un accès par téléphone à un service offert par un réseau de télécommunication l'accès utilisant un jeu (SUB1) de données (PIN1, IMSI1, MSISDN) d'identification stockées dans un module d'identification (SIM), l'accès au service étant bloqué (Bl) en réponse à un événement (WPIN3) ou en absence d'événement (PIN).

L'invention prévoit d'utiliser un jeu supplémentaire (SUB2) de données (INSI2, MSISDN) d'identification stockées dans le module d'identification (SIM) et/ ou prévoit un mode de communication restreint (Com SC) pour établir une communication avec un centre de maintenance (SC) lorsque l'accès est bloqué, afin de permettre un déblocage à distance de l'accès au service.



FR 2 763 773 - A1

DEBLOCAGE A DISTANCE D'ACCES A UN SERVICE DE TELECOMMUNICATION

La présente invention concerne le domaine des systèmes de d'accès à des services disponibles sur des réseaux téléphoniques, notamment les systèmes d'accès codé à des services de communication par téléphone mobile.

De tels systèmes d'accès à des services téléphoniques prévoient un contrôle du numéro d'abonnement au service ainsi qu'un contrôle du code secret d'un utilisateur de l'abonnement, ce qui évite l'utilisation du service téléphonique par des tiers non autorisés.

La figure 1 illustre par exemple un système de type connu dans lequel un poste de téléphone mobile 1 est en liaison radiotéléphonique avec un réseau téléphonique PN. Le téléphone mobile 1 fonctionne généralement avec un dispositif standard anti-fraude, par exemple avec un module d'identification d'abonnement SIM enfichable (carte à puce).

Un premier rôle des dispositifs anti-fraude connus consiste à faire reconnaître le numéro d'abonnement du téléphone mobile utilisé pour que les communications du poste téléphonique soient autorisées. Par exemple, le module d'identification de l'abonnement SIM élabore un message d'identification crypté qui permet au réseau PN, notamment à une station de retransmission 2 du réseau, de reconnaître le numéro d'abonnement du téléphone mobile utilisé.

Le téléphone mobile 1 émet régulièrement des messages d'identification pendant son fonctionnement, en veille ou en mode actif, pour signaler sa présence dans la zone de couverture (appelée cellule) d'une station 2. La localisation et l'identification du téléphone mobile 1 permet au réseau d'acheminer les communications destinées au téléphone mobile ou issues du téléphone mobile, via la station de retransmission 2 la plus adaptée. L'identification de l'abonnement permet d'éviter les fraudes, un autre téléphone ne pouvant émettre le même type de message d'identification crypté et utiliser l'abonnement du téléphone mobile 1.

Un second rôle des dispositifs anti-fraude connus consiste à identifier l'utilisateur par son code secret pour éviter l'utilisation du téléphone par des tiers non autorisés. Le téléphone mobile 1 comporte généralement un clavier numérique permettant à l'utilisateur de composer un code d'identification personnel PIN et d'accéder aux services de son poste téléphonique 1.

Les dispositifs standards anti-fraude prévoient un blocage définitif de l'accès à un téléphone mobile 1 après un nombre limité d'essais de composition de code d'identification personnel PIN, ces essais étant généralement limités au nombre de trois.

Plus généralement, des services disponibles sur les réseaux téléphoniques prévoient des accès codés avec des procédures de blocage en cas d'erreurs de code ou en fin d'abonnement au service.

Un inconvénient des systèmes d'accès codé à des services disponibles sur un réseau de communication par

téléphone à accès codé est que le déblocage de l'accès ne peut se faire que par la transmission à l'utilisateur par la prestataire de service d'un code de déblocage et d'une procédure dépendant du téléphone utilisé. Notamment avec le nombre croissant d'utilisateurs de téléphones mobiles, et la complication des codes d'identification personnel s'ensuivant, les essais erronés de codes d'identification personnel et les blocages de postes téléphoniques deviennent de plus en plus fréquents. Le déblocage des téléphones mobiles crée une surcharge pour le prestataire de service et une frustration des utilisateurs.

Un but de la présente invention est de réaliser un système d'accès codé à des services disponibles sur un réseau de communication par téléphone, supprimant les inconvénients précités, tout en conservant une sûreté élevée de dispositif anti-fraude.

Succinctement, ce but est atteint en réalisant un système de déblocage de l'accès à un service disponible sur un réseau téléphonique, le déblocage de l'accès étant effectué par communication téléphonique avec un service de maintenance, les communications du téléphone de l'utilisateur pendant le blocage, étant simplement restreintes au service de maintenance ou accessibles par un autre code d'abonnement.

Un avantage du système de déblocage d'accès selon l'invention est qu'il permet un déblocage d'accès à distance puisque le téléphone peut encore communiquer avec le centre de maintenance lorsqu'il est bloqué.

Selon l'invention, il est prévu un procédé de déblocage d'accès à un service disponible sur un réseau

de communication par téléphone, ledit accès mettant en oeuvre des étapes d'identification utilisant un jeu de données d'identification stockées dans un module d'identification, l'accès étant bloqué en réponse à un événement ou en l'absence d'événement, l'accès étant débloqué en chargeant des commandes de déblocage auprès du module d'identification, caractérisé en ce qu'il comporte des étapes consistant à :

- prévoir un jeu supplémentaire de données d'identification stockées dans le module d'identification, et

- établir une communication entre le téléphone et un centre de maintenance en utilisant le jeu supplémentaire lorsque l'accès est bloqué, afin de permettre un déblocage à distance de l'accès au service du réseau.

En outre, l'invention prévoit un autre procédé de déblocage d'accès à un service disponible sur un réseau de communication par téléphone, ledit accès mettant en oeuvre des étapes d'identification utilisant un jeu de données d'identification stockées dans un module d'identification, l'accès étant bloqué en réponse à un événement ou en l'absence d'événement, l'accès étant débloqué en chargeant des commandes de déblocage auprès du module d'identification, caractérisé en ce qu'il comporte des étapes consistant à :

- prévoir un mode restreint de communications, toute communication à partir du téléphone étant restreinte à un centre de maintenance selon ledit mode, et

- mettre en oeuvre le mode restreint de communication lorsque l'accès est bloqué, afin de

permettre un déblocage à distance de l'accès au service du réseau.

L'invention s'applique particulièrement au déblocage du code d'accès à un service de communication par téléphone mobile.

Selon l'invention, il est prévu un dispositif d'accès déblocable à un service disponible sur un réseau de communication par téléphone, le dispositif comportant des moyens d'identification d'abonnement permettant d'accéder au service du réseau par communication téléphonique en transmettant un jeu de données d'identification, l'accès étant bloqué en réponse à un événement ou en l'absence d'événement caractérisé en ce que, lorsque l'accès est bloqué, les moyens d'identification transmettent un jeu supplémentaire de données d'identification et permettent d'accéder à un centre de maintenance par communication téléphonique, les communications du téléphone étant restreintes au centre de maintenance lorsque le jeu supplémentaire de données est transmis, afin de permettre un déblocage à distance de l'accès au service du réseau.

Il est prévu, que le centre de maintenance transmet à distance et/ou automatiquement des commandes de déblocage, de préférence selon un service de messages condensés de commandes.

L'invention prévoit encore une carte à puce d'identification d'abonnement permettant un accès déblocable à un service disponible sur un réseau de communication par téléphone, la carte comportant :

- des moyens de stockage d'au moins un jeu de données d'identification,

caractérisée en ce qu'elle comporte :

- des moyens apte à établir des communications restreintes avec un centre de maintenance et,

- des moyens pour charger et effectuer des commandes de déblocage d'accès.

D'autres caractéristiques, buts et avantages de la présente invention apparaîtront à la lecture de la description et des dessins ci-après, donnés uniquement à titre d'exemples non limitatifs ; sur les dessins annexés :

- La figure 1 précédemment décrite, représente un système de téléphone mobile à accès codé de type connu;

- La figure 2 schématise un déblocage d'accès à un service téléphonique selon l'invention ;

- La figure 3 schématise les étapes d'un processus de déblocage d'accès à un service téléphonique selon l'invention ; et,

- La figure 4 représente une carte à puce permettant un accès déblocable à un service téléphonique selon l'invention.

Un système de téléphone mobile apte à mettre en oeuvre l'invention comporte des moyens d'identification d'abonnement SIM. Ces moyens SIM peuvent être implantés sur une carte de circuit imprimé enfichable dans le bloc de téléphone mobile 1 comme visible à la figure 1.

Selon un mode de réalisation préféré de l'invention, il est prévu que les moyens d'identification d'abonnement SIM sont implantés sur une carte à puce ou tout support portatif à microprocesseur et mémoire, constituant un circuit électronique complémentaire du téléphone mobile, le téléphone mobile 1 comportant par exemple un lecteur de

carte à puce. Ce mode de réalisation préféré sera détaillé par la suite.

Divers modes équivalents de réalisation des moyens d'identification d'abonnement sont à la portée de l'homme du métier et ne seront pas détaillés dans la présente. Seules les fonctionnalités des circuits électroniques prévues conformément à l'invention seront détaillées ci-après.

Le fonctionnement normal d'un système de téléphone à accès déblocable à distance est illustré en partie gauche de la figure 3 par les étapes 0 à 99. Les échanges de données prévus pendant le fonctionnement normal sont illustrées également aux six dernières lignes de la figure 2.

En détail, l'étape 0 de début correspond à la mise en fonctionnement du téléphone mobile 1, c'est-à-dire la mise sous tension avant toute communication radio-téléphonique. Le système de téléphone mobile commence un processus d'identification, de préférence dès sa mise en fonctionnement, de sorte que la station 2 de retransmission de la cellule où il se trouve reconnaisse son numéro d'abonnement (MSISDN) et puisse lui adresser les appels téléphoniques qui lui sont destinés.

Pour cela, comme illustré figure 2, le système de téléphone mobile 1 va émettre un message crypté SUB1, à partir d'un jeu de données, à destination de la station 2 locale du réseau PN de téléphone, le jeu de données étant reconnaissable par décryptage au niveau de la station 2. Le décryptage du message SUB est effectué de préférence par un centre serveur CC relié à la station 2 recevant le message crypté SUB1 de données cryptées.

Le système de téléphone mobile comporte à cette fin des moyens d'identification d'abonnement SIM, stockant et mettant en oeuvre des données d'identification et des algorithmes de cryptage, les données mémorisées permettant, d'une part que le téléphone mobile reconnaisse un utilisateur US et d'autre part que le téléphone mobile 1 se fasse reconnaître par le réseau PN.

Comme visible au bas de la figure 2 dans une étape d'identification Id, dès la mise en fonctionnement OFF-ON, les moyens d'identification SIM demandent à l'utilisateur US de rentrer un code d'identification personnel PIN. Dans l'étape Id, les moyens d'identification d'abonnement SIM comparent le code PIN entré par l'utilisateur et le code PIN1 stocké en mémoire. Lorsque le code PIN entré est valide, le système de téléphone mobile 1 passe à une étape d'identification de l'abonnement, les moyens d'identification d'abonnement étant dans un état débloqué Un. Au début de cette étape Un, le téléphone mobile émet un message crypté SUB1 de données correspondant à l'identification de l'abonnement de téléphone mobile. Les messages cryptés SUB émis par le téléphone changnet à chaque étape d'identification pour ne pas être imités. Un message crypté SUB1 est élaboré par les moyens d'identification d'abonnement SIM du téléphone 1 à partir de données en mémoires, telles qu'un numéro IMSI1 identificateur d'abonnement de téléphone mobile et d'une clé K1 secrète de cryptage numérique.

Un mode de réalisation préféré d'algorithme de fonctionnement des moyens d'identification d'abonnement

et de blocage d'accès à un service téléphonique selon l'invention est schématisé sur la figure 3. Le processus normal d'identification de l'utilisateur et d'identification de l'abonnement est détaillé aux étapes 10,20,30,40 et 50.

A l'étape 10, des moyens SIM consultent l'indicateur Bl d'état de blocage. Si le système est dans un état débloqué Un, par exemple si l'indicateur Bl a une valeur nulle, les moyens d'identification d'abonnement SIM passent à l'étape 20 et demandent à l'utilisateur son code d'identification personnel PIN. Si le code PIN1 valide est composé, le système passant aux étapes 40 et 50 émet le message crypté SUB1 d'identification d'abonnement. Lorsque la station de transmission 2 locale et le centre serveur CC décryptent le message SUB1 avec la clé secrète K1 et reconnaissent le numéro IMSI1 identificateur d'abonnement, le système de téléphone mobile est prêt à communiquer. Plus précisément, une base de données DB du centre de maintenance SC stocke le numéro MSISDN d'abonnement de téléphone mobile sous le numéro identificateur IMSI1, avec la zone de localisation LOC, de façon à pouvoir acheminer un appel destiné au téléphone mobile 1 via la station de retransmission 2 la plus adaptée. Notons que le téléphone 1 est identifié et localisé en permanence même lorsqu'il est en état de veille, de sorte qu'un appel puisse lui être acheminé.

Si le code PIN composé est erroné, le système comptabilise cette erreur à l'étape 70 en incrémentant un compteur CPTR. Tant que le compteur CPTR a une valeur inférieure à trois selon l'exemple de l'étape

80, le système redemande son code PIN à l'utilisateur en revenant à l'étape 20.

Lorsque trop d'essais infructueux ont été successivement effectués, par exemple quand le compteur CPTR a une valeur supérieure ou égale à trois, le système passe dans un état bloqué Bl, la valeur de l'indicateur Bl étant mise à 1, à l'étape 90.

Autrement, après le succès des étapes 10, 20, 30, 40 et de l'étape 50 d'identification d'abonnement par émission de message crypté SUB1, l'utilisateur peut effectuer des communications étendues Gen Com qu'il désire (étape 60). Il est notamment prévu que l'étape 20 de composition du code PIN1 n'est pas répétée lors des communications ultérieures de l'utilisateur, les étapes 20 et 30 d'identification Id étant effectuée seulement à la mise en fonctionnement du système.

Le blocage du système intervient dans l'exemple de fonctionnement de l'algorithme de la figure 3, après que trois essais de codes infructueux ont été effectués et que l'indicateur d'état Bl est mis à une valeur 1 à l'étape 90. L'accès aux communications est alors impossible, le système de téléphone mobile 1 stockant dans une mémoire non effaçable la valeur 1 de l'indicateur d'état Bl. A chaque remise en fonctionnement du système, l'accès à l'étape 60 de communication normale est interdit, l'état de blocage Bl=1 étant reconnu dès la première étape 10.

L'invention prévoit cependant des possibilités de communication lorsque le système est en état bloqué Bl, après avoir dépassé le nombre limité d'essais par exemple.

Une première possibilité, selon l'invention, prévoit que le système utilise un jeu supplémentaire de données d'identification d'abonnement pour entrer en communication avec un centre de maintenance avec cet abonnement de secours.

Une deuxième possibilité, selon l'invention, prévoit que le système entre en mode restreint de communication avec le centre de maintenance.

Ces deux possibilités sont combinées dans l'exemple de la figure 2.

Sur la figure 2, on a représenté par colonnes et par lignes se succédant chronologiquement, les opérations de l'utilisateur US, l'état St et les opérations des moyens d'identification SIM, les opérations du centre de maintenance SC et le contenu de la base de données DB ainsi que les échanges téléphoniques entre l'utilisateur US, les moyens d'identification SIM du téléphone mobile, le centre de maintenance SC et un correspondant sur le réseau PN.

Les premières lignes de la figure 2 montrent un exemple de mise en fonctionnement OFF-ON du téléphone mobile suivi de trois lignes Id d'identification. Dans le cas de la figure 2, les moyens SIM demandent trois fois le code PIN et l'utilisateur compose successivement trois codes erronés WPIN1, WPIN2 et WPIN3. Le système passe donc dans un état St bloqué Bl. Ensuite, une fois que l'utilisateur a interrompu ON-OFF et remis en fonctionnement OFF-ON le poste de téléphone mobile 1, le système passe en mode de communication restreint Re. Les moyens d'identification de l'abonnement SIM envoient alors le jeu supplémentaire

SUB2 de données IMSI2, K2 sous forme de message crypté SUB au centre serveur SC du réseau PN.

La partie droite de l'algorithme de la figure 3 illustre un exemple de fonctionnement des moyens d'identification de l'abonnement pendant une phase de blocage.

On voit qu'après l'étape 90 où l'indicateur B1 prend la valeur 1, l'utilisateur peut seulement effectuer une remise en fonctionnement du poste de téléphone mobile 1. L'algorithme enchaîne alors automatiquement l'étape de début 0, puis les étapes 10 et 100, de test de B1 et de F1. Comme l'indicateur d'état B1 a une valeur 1 et en admettant qu'un autre indicateur d'état F1, dont le rôle sera explicité par la suite, a une valeur nulle, l'algorithme passe à l'étape 110 qui prévoit selon l'invention, que les moyens d'identification SIM du téléphone mobile 1 transmettent au réseau de téléphone PN un message SUB crypté à partir du jeu supplémentaire SUB2 de données.

L'utilisation du jeu supplémentaire SUB2 de données SUB2 particulier va permettre au réseau PN et au centre de maintenance SC de reconnaître l'état bloqué du système tout en identifiant l'abonnement du téléphone mobile.

Pour cela il est prévu que le second message crypté SUB soit calculé par l'algorithme de cryptage à partir d'un jeu supplémentaire SUB2 de données, comportant par exemple le même numéro d'abonnement de téléphone mobile MSISDN, un autre numéro IMSI2 identificateur et une autre clé K2 secrète de cryptage par rapport au jeu SUB1 de données MSISDN, IMSI1, K1 utilisé normalement, à l'état débloqué.

Le jeu supplémentaire SUB2 de données du message SUB peut être envoyé automatiquement au centre de maintenance SC sans que l'utilisateur n'intervienne. Le numéro téléphonique N°SC du centre de maintenance SC est dans ce cas stocké par les moyens d'identification d'abonnement SIM. On peut aussi prévoir que le centre de maintenance SC n'effectue pas la commutation des numéros téléphoniques composés par l'utilisateur quand le jeu supplémentaire SUB2 de données est envoyé, mais entre automatiquement en communication avec l'utilisateur.

Le centre de maintenance SC décrypte donc les messages qu'il reçoit avec la seconde clé K2, les deux clés K1 et K2 secrètes étant stockées dans la base de données DB sous le numéro d'abonnement de téléphone mobile MSISDN pour faciliter le décryptage des messages reçus. Le jeu supplémentaire SUB2 de données d'identification sert en quelque sorte de jeu de secours lorsque les communications normales sont bloquées.

Il est prévu que le jeu supplémentaire SUB2 de données du message SUB permet d'accéder seulement au centre de maintenance SC, les communications étant restreintes à ce centre lorsque le système est en état bloqué Bl=1.

L'utilisateur peut alors entrer en communication uniquement avec le centre de maintenance SC, selon le mode restreint de communication Re, quel que soit le numéro de téléphone composé.

Un opérateur du centre SC ou un processus d'interrogation automatique interroge alors

l'utilisateur pendant une telle communication Com SC, en mode restreint Re

Le centre de maintenance SC peut alors envoyer les commandes Ins, Dat permettant de rétablir le fonctionnement normal du système de téléphone mobile 1.

Lors de telles communications téléphoniques restreintes, le mode de réalisation préféré de l'invention prévoit que le centre de maintenance SC envoie des instructions Ins et des données Dat de déblocage de l'accès codé. De préférence les instructions Ins permettent de mettre en oeuvre un code PUK1 de déblocage contenu en mémoire (non accessible extérieurement) des moyens d'identification d'abonnement SIM. Toutefois, le code PUK1 de déblocage peut aussi être communiqué directement par le centre de maintenance SC parmi les données Dat de déblocage. L'ensemble de ces instructions Ins, données Dat et code PUK1 de déblocage est généralement désigné sous le nom de commandes de déblocage.

Une première variante de réalisation prévoit que l'accès au service téléphonique est débloqué simplement par la fourniture du code de déblocage PUK1.

Une seconde variante de réalisation de l'invention prévoit que l'envoi des commandes de déblocage par le centre de maintenance SC entraîne la levée d'un drapeau, l'indicateur d'état Fl étant mis à une valeur 1 à une étape 130. Ce drapeau signale que le déblocage du système est en cours. Le déblocage du système commence alors à la remise en fonctionnement OFF/ON du système en suivant les étapes 0, 10, 100 et 140 du processus de la figure 3.

De préférence, l'indicateur d'état Fl du système de téléphone mobile 1 est mis à une valeur 1 par le centre de maintenance SC qui envoie une instruction Ins correspondant à la levée du drapeau.

L'algorithme de fonctionnement du système de téléphone mobile peut comporter aussi une étape 130 de mise à la valeur 1 de l'indicateur Fl après la fin d'une communication avec le centre de maintenance SC à l'étape 120.

Une étape 100 de test de l'indicateur Fl est alors prévue, comme visible dans l'algorithme figure 3.

Ainsi, le système 1 entre en communication restreinte avec le centre de maintenance SC, suivant les étapes 110, 120, 130 et 139, seulement si l'indicateur Fl a une valeur nulle, c'est-à-dire si l'utilisateur n'a pas encore communiqué avec le centre de maintenance SC.

Après vérification à l'étape 120 de l'identité de l'utilisateur et envoi des commandes Ins, Dat, et éventuellement PUK1 de déblocage, on peut prévoir que le déblocage du système commence directement à une étape 140. L'algorithme de la figure 3 prévoit cependant une variante dans laquelle l'utilisateur doit interrompre le fonctionnement du téléphone mobile à une étape 139 avant que le déblocage du système ne commence à l'étape 140.

Ainsi, après la communication ComSC avec le centre de maintenance SC et de préférence après remise en fonctionnement du téléphone mobile, le système constatant que les indicateurs Bl et Fl ont des valeurs 1, demande le code PUK de déblocage d'accès à l'étape 140. A l'étape 150, le système vérifie le code PUK

chargé (ou composé par l'utilisateur) par rapport à une valeur PUK1 de code stockée en mémoire.

Si le code de déblocage PUK est erroné, le système reste dans un état St bloqué (Bl=1) à l'étape 159.

Après la validation du code PUK, l'algorithme peut comporter une étape 160 dans laquelle l'utilisateur introduit une valeur de code newPIN d'identification personnelle de son choix en guise de code d'identification personnel PIN. Cette valeur newPIN de code d'identification sera stockée par les moyens d'identification d'abonnement SIM pour toutes les étapes ultérieures 20, 30 de vérification de code d'identification personnel. Les indicateurs d'état Fl et Bl sont évidemment remis à des valeurs nulles aux étapes 170 et 180 avant la fin 189 de la procédure de déblocage. Après extinction du téléphone mobile, le fonctionnement normal reprend en passant par les étapes 0, 10, 20, 30 et suivantes.

L'invention prévoit de préférence que les communications en mode restreint sont effectuées sur des canaux de transmissions particuliers comme des canaux de service de messages condensés de type canaux SMS.

De tels canaux de service sont utilisés par les prestataires de services pour accéder au poste de téléphone mobile et l'interroger, effectuer des opérations numériques ou envoyer des instructions.

Un service de message condensé décrit dans le brevet FR 2 704 704 permet notamment de disposer d'un jeu réduit d'instructions, instructions ayant donc un codage simple et court. Le jeu réduit d'instructions comporte les instructions d'opération les plus

courantes, les opérations particulières étant exécutées après une instruction spéciale et le chargement des données et codes d'exécution correspondant à chaque opération particulière.

L'utilisation d'un tel service de message condensé lors des communications entre le centre de maintenance et le système de téléphone mobile est particulièrement avantageuse pour un déblocage rapide du système. Le canal de service de message condensé permet l'envoi des instructions Ins, des données Dat et, éventuellement, des codes PUK de déblocage d'accès. Les échanges d'informations entre l'utilisateur et le centre de maintenance peuvent utiliser le canal vocal ou s'établir automatiquement entre le système de téléphone mobile 1 et le centre serveur SC par le canal des messages condensés.

L'avantage de l'utilisation de tels canaux de service est la possibilité d'automatiser la procédure de déblocage à distance du code d'accès, le centre de maintenance traitant informatiquement les demandes des utilisateurs et envoyant les commandes de déblocage sous forme de commandes condensées pour une plus grande rapidité.

L'invention permet encore une amélioration sensible du confort d'utilisation du téléphone mobile en prévoyant qu'un poste de téléphone mobile 1 est livré à l'état bloqué initialement, c'est-à-dire qu'il entre automatiquement en mode de communication restreint Re avec le centre de maintenance à la première utilisation.

L'utilisateur est alors en communication avec un opérateur qui peut éventuellement lui communiquer

oralement son code de déblocage d'accès PUK, et lui détailler la procédure d'entrée de code à effectuer pour la réinitialisation du code d'identification personnel PIN. Cette variante avantageuse peut permettre aussi au système d'enregistrer un code newPIN d'identification personnel au choix de l'utilisateur dès la première mise en service.

L'implantation des moyens d'identification d'abonnement selon l'invention sur un système de téléphone mobile peut être réalisée sous forme de carte de circuit électronique imprimé enfichable dans le bloc de téléphone mobile.

Un deuxième mode de réalisation consiste à prévoir que les moyens d'identification d'abonnement sont implantés sur une carte à puce, le bloc de téléphone mobile disposant d'un transcripteur de données sur carte à puce encore appelé lecteur.

Un avantage de ce deuxième mode de réalisation est de permettre à plusieurs utilisateurs d'effectuer des communications à partir d'un poste de téléphone mobile quelconque, chaque utilisateur étant identifié par la carte à puce et le code d'accès qu'il compose et son abonnement téléphonique étant authentifié par les données stockées en mémoire de la carte à puce.

La figure 4 illustre une configuration possible du circuit électronique appelé puce d'une telle carte SimCard. Le circuit comporte de préférence un microprocesseur CPU pour la mise en oeuvre d'un programme OS de fonctionnement dont les instructions sont stockées en mémoire morte ROM, les instructions et données temporaires étant stockées en mémoire vive RAM.

La réalisation d'un tel circuit électronique classique ne sera pas détaillée ici.

Une particularité d'une carte à puce d'identification d'abonnement permettant un accès déblocable à un service téléphonique selon l'invention est de comporter des moyens aptes à établir des communications restreintes avec le centre de maintenance. Par exemple, une mémoire morte reprogrammable EEPROM comporte un programme OSA, le numéro téléphonique N°SC du centre de maintenance SC et éventuellement le code de déblocage d'accès PUK1.

De préférence, une carte à puce SIMCard permettant un accès déblocable selon l'invention stocke, notamment en mémoire morte reprogrammable EEPROM, un jeu normal SUB1 et un jeu supplémentaire SUB2 de données d'identification IMSI1, K1, IMSI2, K2, MSISDN destinés à l'émission de messages cryptés d'identification SUB selon le mode débloqué ou bloqué du système.

La mémoire EEPROM peut encore contenir une zone mémoire pour stocker la valeur des indicateurs d'état B1, F1 précités ou des indicateurs équivalents Id, B1, Re, Un, F1 dont la valeur est modifiée lors des modes d'identification, bloqué, communication restreinte, débloqué et déblocage en cours, respectivement.

L'invention a été exposée précédemment en suivant l'exemple d'un déblocage d'accès à un service de communication téléphonique mobile suite à l'introduction de codes erronés d'identification personnelle. Cependant, l'invention peut être généralisée au déblocage d'accès à tout service disponible sur un réseau de communication par téléphone, le blocage d'accès ayant lieu suite à un

événement ou à une absence d'événement. Par événement, on entend tout événement connu de l'homme de l'art conduisant à un blocage de l'accès à un service offert par un réseau de télécommunication, par exemple une fin des droits d'accès à un abonnement temporaire, ou le solde d'un service prépayé, ou encore une panne d'accès à un service offert par un réseau de communication, panne due soit à la carte à puce, soit au réseau ou autre, pourvu que le jeu supplémentaire de données d'abonnement permette l'accès au service. Ce type de panne d'accès se produit en cas de surcapacité sur un réseau de communication, ou en cas de problème d'initialisation d'un téléphone mobile pendant le routage (roaming) de communications internationales.

D'autres modes de réalisation, caractéristiques et avantages de l'invention apparaîtront à l'homme de métier sans sortir du cadre des revendications ci-après.

REVENDICATIONS

1. Procédé de déblocage d'un accès par téléphone (1) à un service offert par un réseau (PN) de télécommunication, ledit accès mettant en oeuvre des étapes d'identification (Id) utilisant un jeu (SUB1) de données (PIN1, IMSI1, MSISDN) d'identification stockées dans un module d'identification (SIM), l'accès étant bloqué (Bl) en réponse à un événement (WPIN3) ou en l'absence d'événement (PIN), l'accès étant débloqué (Un) en chargeant des commandes (Ins, Dat) de déblocage auprès du module d'identification (SIM), caractérisé en ce qu'il comporte des étapes consistant à :

- prévoir un jeu supplémentaire (SUB2) de données (IMSI2, MSISDN) d'identification stockées dans le module d'identification (SIM), et
- établir une communication (Com SC) entre le téléphone (1) et un centre de maintenance (SC) en utilisant le jeu supplémentaire (SUB2) lorsque l'accès est bloqué (Bl), afin de permettre un déblocage à distance de l'accès au service du réseau.

2. Procédé de déblocage d'un accès par téléphone (1) à un service offert par un réseau (PN) de télécommunication, ledit accès mettant en oeuvre des étapes d'identification (Id) utilisant un jeu (SUB1) de données (PIN1, IMSI1, MSISDN) d'identification stockées dans un module d'identification (SIM), l'accès étant bloqué (Bl) en réponse à un événement (WPIN3) ou en l'absence d'événement (PIN), l'accès étant débloqué (Un) en chargeant des commandes (Ins, Dat) de déblocage

auprès du module d'identification (SIM), caractérisé en ce qu'il comporte des étapes consistant à :

- prévoir un mode (Re) restreint de communications, toute communication (Com SC) à partir du téléphone (1) étant restreinte à un centre (SC) de maintenance selon ledit mode (Re), et

- mettre en oeuvre le mode (Re) restreint de communication lorsque l'accès est bloqué (Bl), afin de permettre un déblocage à distance de l'accès au service du réseau.

3. Procédé selon l'une des revendications précédentes, caractérisé par une étape supplémentaire consistant à :

- charger les commandes (Ins, Dat) de déblocage lors de ladite communication (Com SC) avec le centre (SC) de maintenance.

4. Procédé selon l'une des revendications précédentes, caractérisé en ce que le centre (SC) de maintenance est apte à transmettre des commandes selon un service de messages condensés (SMS) de commandes.

5. Procédé selon l'une des revendications précédentes, caractérisé en ce que ledit accès met en oeuvre des étapes d'identification (Id) d'un utilisateur (Us) du service, au moins un jeu (SUB1, SUB2) de données d'identification comportant un code (PIN1) d'identification personnelle de l'utilisateur (Us).

6. Procédé selon la revendication précédente, caractérisé en ce que le code (PIN1) d'identification personnel est modifié lors d'une communication (Com SC) avec le centre (SC) de maintenance.

7. Procédé selon l'une des revendications précédentes, caractérisé en ce que plusieurs modules d'identifications (SIM) stockent des jeux supplémentaires (SUB2) de données d'identification comportant des données (IMSI2, K2) identiques.

8. Procédé selon l'une des revendications précédentes, caractérisé en ce que l'accès au service (Gen Com) est initialement bloqué (Bl) pour un nouvel utilisateur (Us) et que l'utilisateur entre directement en communication (Com SC) avec le centre (SC) de maintenance.

9. Dispositif d'accès déblocable par téléphone (1) à un service offert par un réseau (PN) de télécommunication, le dispositif comportant des moyens (SIM) d'identification d'abonnement, les moyens d'identification comportant un jeu (SUB1) et un jeu supplémentaire (SUB2) de données d'identification, les moyens d'identification étant aptes à transmettre le jeu (SUB1) de données (PIN1, IMSI1, MSISDN) pour accéder au service par communication téléphonique, l'accès étant bloqué en réponse à un événement (WPIN3) ou en l'absence d'événement (PIN) caractérisé en ce que, lorsque l'accès est bloqué, les moyens (SIM) d'identification sont aptes à transmettre le jeu supplémentaire (SUB2) de données (IMSI2, MSISDN) pour accéder à un centre de maintenance par communication téléphonique, les communications du téléphone (1) étant restreintes au centre de maintenance (SC) lorsque le jeu supplémentaire (SUB2) de données est transmis, afin de permettre un déblocage à distance de l'accès au service du réseau.

10. Dispositif d'accès déblocable par téléphone (1) à un service offert par un réseau de télécommunication, le dispositif comportant des moyens (SIM) d'identification, les moyens d'identification comportant un jeu (SUB1) et un jeu supplémentaire (SUB2) de données d'identification, les moyens d'identification étant aptes à transmettre le jeu (SUB1) de données (PIN1, IMSI1, MSISDN) pour accéder à des communications téléphoniques (Gen Com) étendues (Un) avec le service, l'accès au service étant bloqué (Bl) en réponse à un événement (WPIN3) ou en l'absence d'événement (PIN), caractérisé en ce que les moyens (SIM) d'identification d'abonnement sont aptes à transmettre le jeu supplémentaire (SUB2) de données (IMSI2, MSISDN) pour autoriser des communications (Com SC) restreintes uniquement avec un centre de maintenance lorsque l'accès au service est bloqué, afin de permettre un déblocage à distance de l'accès aux communications étendues (Gen Com).

11. Dispositif selon la revendication 9 ou 10, caractérisé en ce que l'accès est autorisé après fourniture d'un code d'identification personnel (PIN1) aux moyens d'identification et en ce que l'accès est bloqué après fourniture de code erroné (WPIN1, WPIN2, WPIN3) ou en l'absence de fourniture de code.

12. Dispositif selon l'une des revendications 9 à 11, caractérisé en ce que les moyens d'identification d'abonnement (SIM) sont initialement bloqués et en ce que les communications sont restreintes (Re) lors de la première utilisation des moyens d'identification d'abonnement (SIM).

13. Carte à puce d'identification d'abonnement (SIM Card) destinée à être utilisée avec un procédé ou un dispositif selon l'une des revendications précédentes, la carte permettant un accès déblocable à un service disponible sur un réseau de communication par téléphone, la carte comportant :

- des moyens (EEPROM) de stockage d'au moins un jeu (SUB1) de données (IMSI1, K1) d'identification,

caractérisée en ce qu'elle comporte :

- des moyens (OSA, N°SC, SUB2) apte à établir des communications restreintes avec un centre de maintenance et,

- des moyens (CPU, OD, OS, OSA, PUK1) pour charger et effectuer des commandes de déblocage d'accès.

14. Carte à puce selon la revendication précédente, caractérisée en ce que les moyens de stockage (EEPROM) stockent un jeu supplémentaire (SUB2) de données (IMSI2, K2) d'identification pour établir des communications restreintes avec le centre de maintenance.

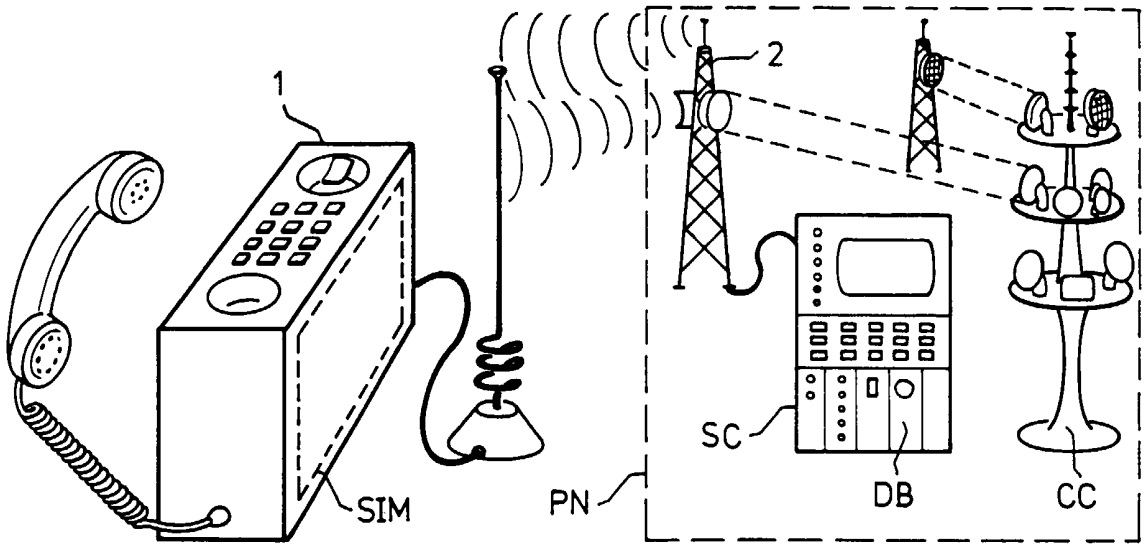

1
2
SIM
PN
SC
DB
CC

Fig. 1

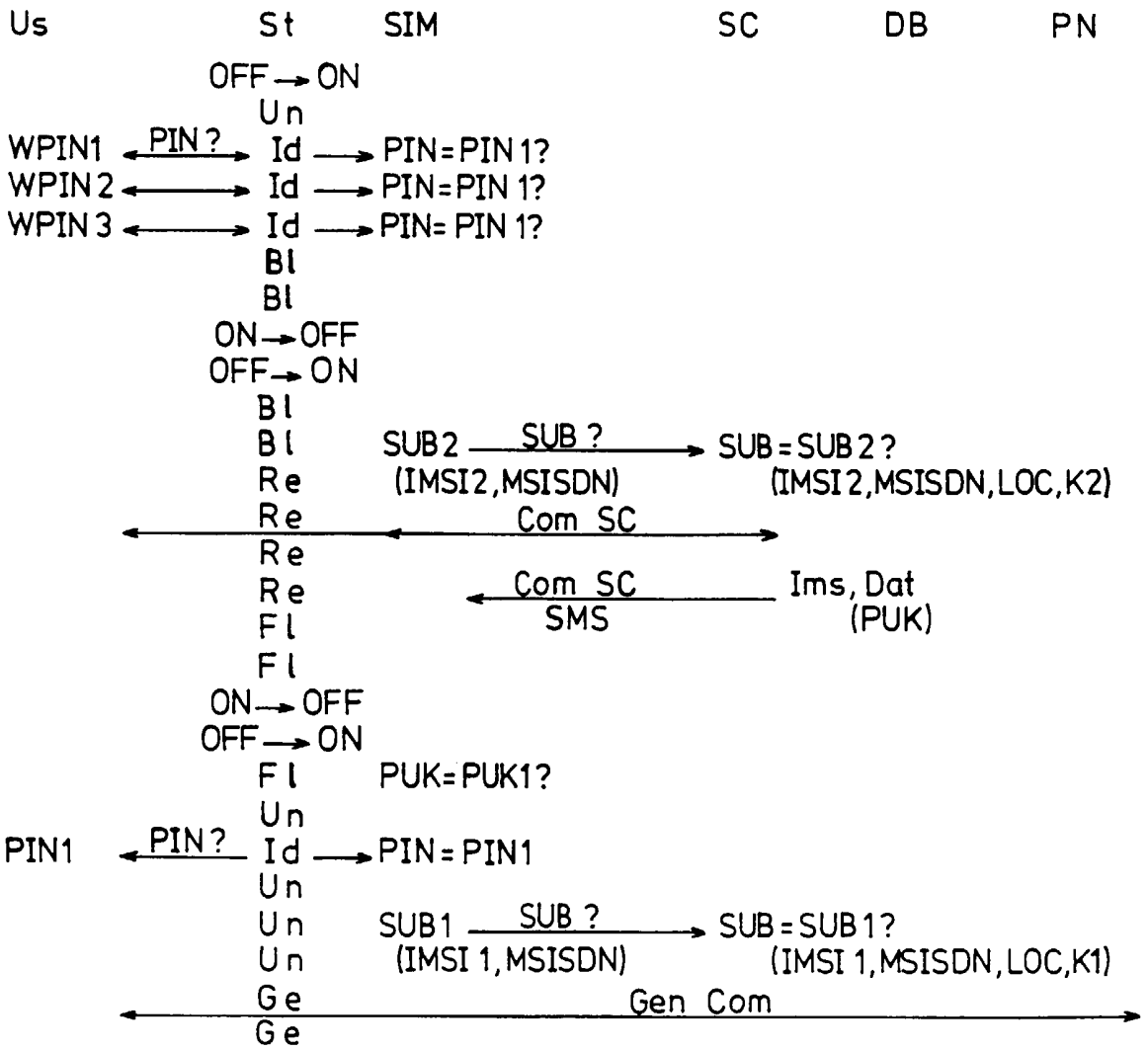

Us
St
SIM
SC
DB
PN
OFF → ON
Un
WPIN1
PIN ?
Id
PIN = PIN 1?
WPIN 2
Id
PIN = PIN 1?
WPIN 3
Id
PIN = PIN 1?
Bl
Bl
ON → OFF
OFF → ON
Bl
Bl
SUB 2
SUB ?
SUB = SUB 2?
Re
(IMSI 2, MSISDN)
(IMSI 2, MSISDN, LOC, K2)
Re
Com SC
Re
Re
Com SC
Ims, Dat
SMS
(PUK)
Fl
Fl
ON → OFF
OFF → ON
Fl
PUK = PUK1?
Un
PIN1
PIN ?
Id
PIN = PIN1
Un
Un
SUB 1
SUB ?
SUB = SUB 1?
Un
(IMSI 1, MSISDN)
(IMSI 1, MSISDN, LOC, K1)
Ge
Gen Com
Ge

Fig. 2

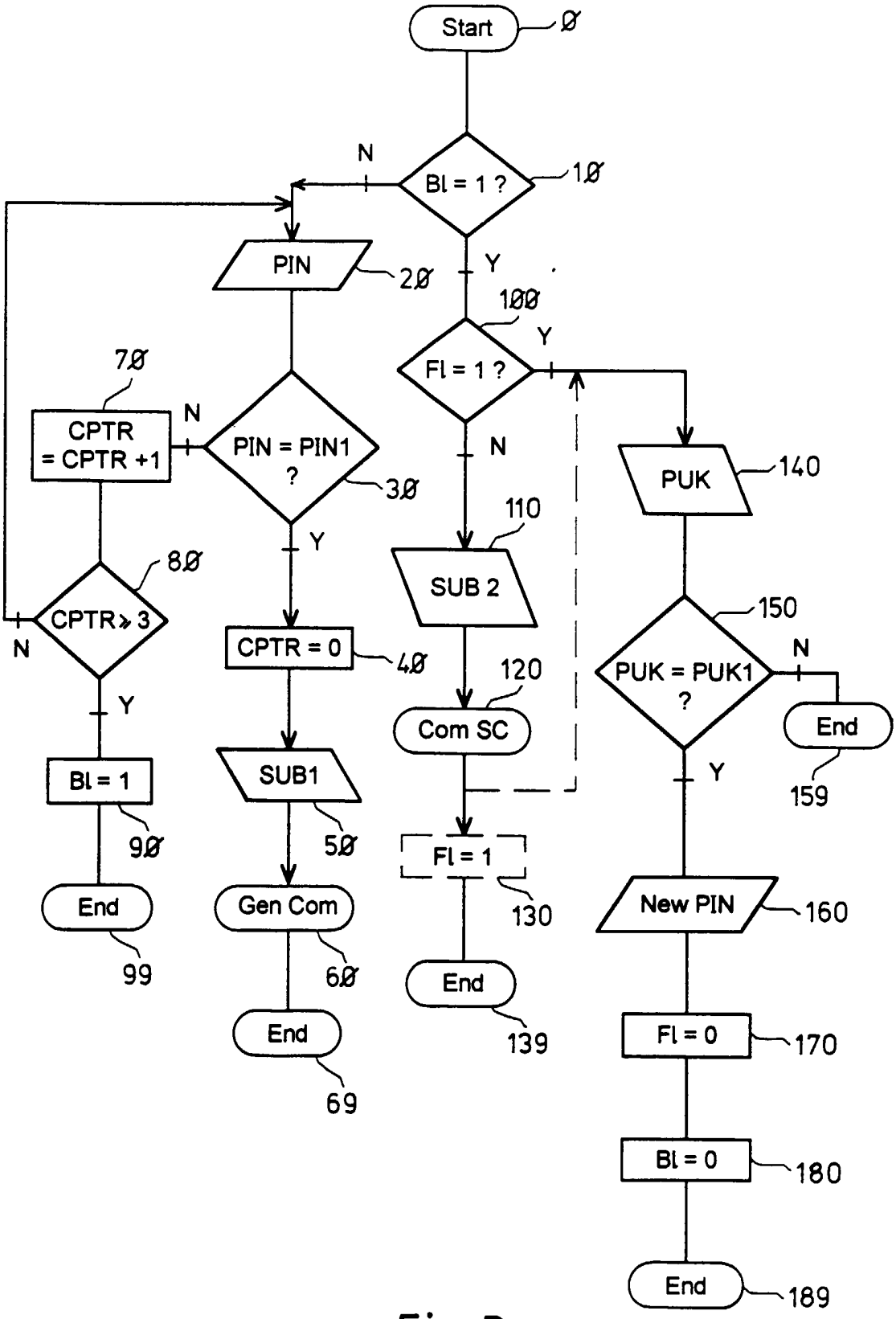

Start
Ø
Bl = 1 ?
1Ø
N
Y
PIN
2Ø
100
Fl = 1 ?
Y
N
7Ø
CPTR
= CPTR +1
N
PIN = PIN1
?
3Ø
Y
PUK
140
110
SUB 2
8Ø
CPTR» 3
N
Y
CPTR = 0
4Ø
120
Com SC
150
PUK = PUK1
?
N
End
159
Y
Bl = 1
9Ø
SUB1
5Ø
Fl = 1
130
New PIN
160
End
99
Gen Com
6Ø
End
139
Fl = 0
170
End
69
Bl = 0
180
End
189

Fig.3

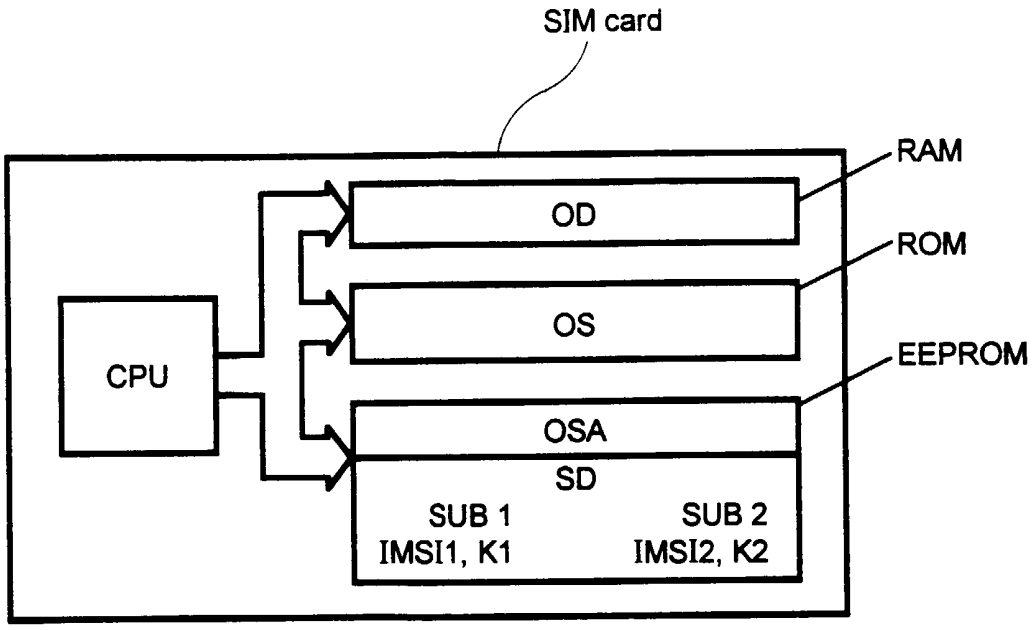

SIM card
RAM
ROM
EEPROM
OD
OS
OSA
SD
CPU
SUB 1
IMSI1, K1
SUB 2
IMSI2, K2

Fig. 4

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 544665
FR 9706428

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
Y	FARRUGIA A J ET AL: "SMART CARD TECHNOLOGY APPLIED TO THE FUTURE EUROPEAN CELLULAR TELEPHONE ON THE DIGITAL D-NETWORK" SELECTED PAPERS FROM THE SECOND INTERNATIONAL SMART CARD 2000 CONFERENCE, 4-6 OCTOBER 1989, AMSTERDAM, NL, 1 janvier 1989, pages 95-107, XP000472724	2-5,8, 10-13
A	* page 102, ligne 15 - ligne 34 *	1,6,9

Y	WO 96 27270 A (ERICSSON GE MOBILE INC ;HENRY RAYMOND C JR (US); SICHER ALAN E (US) * page 16, ligne 23 - page 18, ligne 33; figures *	2-4,8, 10,12,13

Y	US 5 517 554 A (MITCHELL JOHN J ET AL)	2,5,10, 11
A	* colonne 3, ligne 28 - ligne 46 * * colonne 3, ligne 60 - ligne 67 *	6

A	DE 43 17 143 A (DETECON GMBH) * abrégé *	1,9,14

A	EP 0 669 774 A (MANNESMANN AG) * abrégé; figure *	7

DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)

H04Q

Date d'achèvement de la recherche	Examinateur
11 mars 1998	Schut, G

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)