(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
11 octobre 2001 (11.10.2001)

PCT

(10) Numéro de publication internationale
WO 01/75817 A1

(51) Classification internationale des brevets[7] : G07F 7/08

(21) Numéro de la demande internationale :
PCT/FR01/00955

(22) Date de dépôt international : 29 mars 2001 (29.03.2001)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
00/04075 30 mars 2000 (30.03.2000) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **ASCOM MONETEL S.A.** [FR/FR]; Rue Claude Chappe, F-07500 Guilherand-Granges (FR).

(72) Inventeur; et
(75) Inventeur/Déposant *(pour US seulement)* : **DUPUIS, Serge** [FR/FR]; 19, Allée Marilyn Monroe, F-26000 Valence (FR).

(74) Mandataire : **THIBON, Laurent**; Cabinet Michel de Beaumont, 1, rue Champollion, F-38000 Grenoble (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, 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, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, 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, GW, ML, MR, NE, SN, TD, TG).

**Publiée :**
— *avec rapport de recherche internationale*

*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.*

(54) **Title:** METHOD FOR AUTHENTICATING SMART CARDS

(54) **Titre :** PROCEDE D'AUTHENTIFICATION DE CARTES A PUCES

(57) **Abstract:** The invention concerns a method for authenticating smart cards inserted into a terminal adapted to communicate with an authenticating device, comprising steps which consist in: generation of a random number (NA) by the authenticating device; sending (13-1) said random number to the card; computation (13-2) by the card, of a first residual value (VR) of value units stored in the card; sending (24) the first result and an information related to the residual value to the authenticating device; storage (13-4) by the authenticating device, of a second result (R2) taking into account the same data as the first result; and verification (13-5) by the authenticating device of the conformity between the two results.

(57) **Abrégé :** L'invention concerne un procédé d'authentification d'une carte à puce introduite dans un terminal propre à communiquer avec un dispositif d'authentification, comprenant les étapes de : génération d'un nombre aléatoire (NA) par le dispositif d'authentification; envoi (13-1) de ce nombre aléatoire à la carte; calcul (13-2), par la carte, d'un premier résultat (R1) prenant en compte, entre autres, ledit nombre aléatoire et une valeur résiduelle (VR) d'unités de compte mémorisées dans la carte; envoi (24) du premier résultat et d'une donnée liée à la valeur résiduelle au dispositif d'authentification; mémorisation (25) de cette donnée dans le dispositif d'authentification; calcul (13-4), par le dispositif d'authentification, d'un deuxième résultat (R2) prenant en compte les mêmes données que le premier résultat; et vérification (13-5), par le dispositif d'authentification, de la cohérence entre les deux résultats.

WO 01/75817 A1

# PROCÉDÉ D'AUTHENTIFICATION DE CARTES À PUCES

La présente invention concerne le domaine des cartes à puce, qu'il s'agisse de cartes à puce synchrones, c'est-à-dire des cartes à logique câblée dépourvues de microprocesseur, ou de cartes à puce asynchrones qui sont pourvues d'un microprocesseur et qui dialoguent par une liaison série asynchrone avec un lecteur ou terminal. Parmi les applications des cartes synchrones, la plus répandue est celle des cartes prépayées, par exemple, les cartes téléphoniques.

L'invention s'applique plus particulièrement à l'authentification d'une carte lors de son introduction dans un terminal, puis en cours d'utilisation. De telles procédures d'authentification, ou de contrôle de signature, sont généralement effectuées lorsqu'une carte est introduite dans un terminal puis périodiquement pendant que celle-ci reste dans le terminal (par exemple, au cours d'une communication téléphonique au moyen d'une carte prépayée). On se référera ci-après à un exemple d'application à des communications téléphoniques au moyen de cartes prépayées. On notera toutefois que l'invention s'applique plus généralement à tout échange d'informations requérant d'incrémenter ou de décrémenter un compteur présent dans une carte à puce, et mettant en oeuvre un protocole d'authentification de la carte présente dans un terminal.

La figure 1 représente, de façon très schématique, un système d'exploitation de cartes à puce du type auquel se rapporte la présente invention. Un tel système est basé sur l'utilisation d'un terminal 1 destiné à recevoir, pour l'établissement d'une communication avec, par exemple, un central de télécommunication 20, une carte 3 à puce 4, par exemple une carte prépayée. Un équipement de contrôle 2 est intercalé entre le central 20 et la ligne à destination d'un ou plusieurs terminaux. Cet équipement a notamment pour rôle d'autoriser ou non une communication et d'effectuer un contrôle périodique en cours de communication. Le terminal 1 comprend de multiples éléments qui sont, pour une grande part fonction de l'application et de l'implantation du terminal. Par souci de simplification, on ne considérera ci-après que les éléments du terminal qui ont un lien direct avec la présente invention, à savoir ceux qui se rapportent à l'acheminement de signaux entre la puce 4 de la carte 3 et l'équipement 2 ou équivalent, pour authentifier la carte et commander le débit de taxes prépayées sur celle-ci. Bien que la figure 1 se réfère à un système dans lequel l'authentification de la carte est mise en oeuvre par l'équipement de contrôle, on notera qu'une telle authentification peut intervenir dans le terminal ou dans un dispositif en amont de l'équipement 2 par rapport au terminal 1. La communication entre le terminal 1 et la carte 3 s'effectue généralement par l'intermédiaire d'un coupleur électrique 5 IFD. Ce coupleur 5 comporte une fente ou lumière (non représentée) d'introduction de la carte 3 ainsi que des contacts (non représentés) propres à venir en relation électrique avec des bornes d'accès à la puce 4. Ces contacts sont raccordés, côté terminal, aux différents éléments nécessaires au traitement des informations et, notamment, à un microprocesseur 6 communiquant lui-même avec une interface 7 dont le rôle est de mettre en forme les signaux devant transiter par une ligne de communication 8 jusqu'à l'équipement 2 et inversement. Si la ligne 8 est une liaison téléphonique entre le terminal 1 et l'équipement 2, cette liaison est bifilaire. En figure 1, on a représenté une

liaison 9 sortant de l'équipement 2 vers le central 20. Cette liaison est multifilaire et correspond, entre autres, aux liaisons de communication entre l'équipement 2 et le central téléphonique qui communique lui-même avec d'autres centraux (non représentés). L'interface 7 du terminal 1 correspond à ce que l'on désigne habituellement par une interface ligne. Une telle interface comprend notamment un duplexeur pour séparer les signaux émis des signaux reçus par la ligne. Cette interface a le plus souvent également pour rôle de séparer les signaux vocaux contenus dans une bande de fréquences jusqu'à environ 4 kHz des signaux dits supravocaux présents dans une bande de fréquences habituellement comprise entre 12 et 18 kHz et servant à véhiculer des informations autres que la parole sur la ligne bifilaire 8.

La structure et le fonctionnement d'un système de communication tel qu'illustré par la figure 1 sont parfaitement connus et ne seront pas détaillés plus avant. On notera simplement que, parmi les fonctions de gestion des communications téléphoniques et d'authentification des cartes à puce prépayées, la répartition de ces fonctions entre l'équipement de contrôle 2 et le terminal 1 peut varier, en particulier, en fonction de "l'intelligence" que l'on souhaite donner au terminal et de ses possibilités d'alimentation autonome. Les terminaux les plus simples prélèvent leur alimentation directement de la ligne téléphonique sans recourir à une alimentation autonome de type alimentation secteur. Les terminaux les plus "intelligents" gèrent l'ensemble des informations liées au paiement de la communication et se contentent d'envoyer, vers le central, la communication téléphonique proprement dite.

Dans le cas d'une carte à puce synchrone, celle-ci comporte essentiellement un décodeur dont le rôle est de générer, à partir d'une combinaison logique de signaux provenant du microprocesseur 6 du terminal, des signaux de remise à zéro et d'incrémentation d'un compteur ainsi qu'un signal d'écriture dans une mémoire de la puce. Cette mémoire est adressée par un mot délivré par le compteur interne à la puce et le contenu de la

mémoire est généralement lu à destination du terminal 1. Le principe de fonctionnement d'une telle carte synchrone est basé sur une mémoire fonctionnant en accès série, c'est-à-dire que le compteur délivre l'adresse de lecture ou d'écriture dans cette mémoire sur la base d'une incrémentation de l'adresse, chaque mot de la mémoire comprenant un seul bit.

Dans des cartes plus évoluées auxquelles s'applique plus particulièrement la présente invention, la puce 4 intègre des fonctions, dites actives, d'authentification ou de calcul de signature pour éviter une duplication ou un piratage des cartes. Le plus souvent, il s'agit toujours de cartes synchrones, c'est-à-dire en logique câblée. Toutefois, dans certains cas, de telles cartes peuvent être pourvues d'un processeur de calcul. La puce 4 comporte généralement un réseau logique programmable chargé de déterminer les droits d'accès à la mémoire de la puce quand la carte est introduite dans un terminal. Un tel réseau logique programmable sert à effectuer des calculs logiques à partir de données, internes à la carte, et de données, fournies par le terminal et provenant généralement du dispositif d'authentification.

On notera que le protocole d'authentification d'une carte prépayée s'effectue généralement de façon temporellement distincte de l'écriture ou de la lecture dans la mémoire de la carte. Par conséquent, l'échange d'informations entre la carte et le terminal utilise les mêmes contacts que ce soit pour accéder à la mémoire de la carte en lecture ou en écriture ainsi qu'en incrémentation ou décrémentation du compteur, ou pour les protocoles d'authentification de la carte.

Les fonctions d'authentification sont rendues de plus en plus complexes afin d'améliorer leur fiabilité en raison des progrès incessants des fraudeurs. La mise en oeuvre d'un mécanisme de calcul de signature fait généralement appel à un calcul au moyen du réseau logique câblé de la carte à partir de signaux reçus par celle-ci. Le résultat de ce calcul est délivré par la carte au terminal qui le transmet au dispositif d'authen-

tification généralement contenu dans l'équipement de contrôle (2, figure 1) qui le compare alors à un résultat qu'il obtient en interne.

Dans le cas des communications téléphoniques au moyen d'une carte prépayée ou d'une carte de télépaiement, les procédures d'authentification sont effectuées régulièrement au cours de la communication. Dans le cas d'une carte téléphonique prépayée, ces procédures d'authentification sont effectuées, en particulier, avant l'établissement d'une communication téléphonique et après chaque débit d'une unité prépayée sur la carte.

La figure 2 illustre, sous forme d'organigramme simplifié, les principaux échanges d'informations entre une carte téléphonique prépayée et un dispositif d'authentification (dans cet exemple, intégré à l'équipement) pendant une communication. A la figure 2, les différentes étapes illustrées par des blocs ont été réparties en trois colonnes séparées par des traits mixtes selon qu'elles ont lieu ou sont déclenchées essentiellement au sein de l'équipement, du terminal ou de la carte. Pour simplifier la présente description, on suppose que le dispositif d'authentification est contenu dans l'équipement.

Tout commence par l'introduction d'une carte prépayée (bloc 10) dans un terminal. Le terminal qui surveille en permanence une telle introduction la détecte (bloc 11) et, le cas échéant après avoir vérifié au moyen de ses propres circuits un certain nombre d'informations relatives à la carte, établit une connexion (bloc 12) avec l'équipement. L'équipement met alors en oeuvre une première phase d'authentification (bloc 13) pour s'assurer de l'authenticité de la carte prépayée introduite dans le terminal. En figure 2, le bloc d'authentification 13 a été représenté côté équipement pour faire ressortir que la phase d'authentification est contrôlée par l'équipement. Toutefois, pendant l'authentification, on assiste à des échanges entre le dispositif d'authentification et la carte. Un exemple plus détaillé de la phase d'authentification, illustrée globalement par

le bloc 13 à la figure 2, sera décrit ultérieurement en relation avec la figure 3.

En supposant que l'authentification de la carte est confirmée par l'équipement, une communication téléphonique peut s'établir. Le terminal procède à cet établissement à partir du numéro saisi par l'utilisateur (bloc 14 d'établissement de communication). Selon le type de communication téléphonique dont il s'agit, la fréquence de consommation des unités de prépaiement téléphonique varie. Un ordre de consommation d'une unité sur la carte prépayée est déclenché par le terminal, l'équipement, ou le central. Un tel ordre de prélèvement de taxe (bloc 15) est en pratique déclenché dès le début de la communication, puis périodiquement à l'expiration de chaque durée correspondant à une unité prépayée. En effet, les débits de taxes s'effectuent généralement en avance lors des communications téléphoniques. L'enregistrement de la consommation d'une unité téléphonique sur la carte s'effectue par une instruction d'écriture dans la puce de la carte pour décrémenter le nombre d'unités de compte prépayées qu'elle contient. Une telle instruction transite par le terminal qui, le cas échéant, la convertit de manière appropriée pour l'écriture dans la carte. Cette écriture est illustrée en figure 2 par un bloc 16 (VR = VR-1, où VR représente la valeur résiduelle de la carte prépayée en nombre d'unités de compte).

Suite à la décrémentation du compteur, on met en oeuvre une nouvelle procédure d'authentification (bloc 13' d'authentification) par l'équipement. Une telle procédure d'authentification est identique à la procédure mise en oeuvre au début de la communication et s'effectue après chaque consommation d'une taxe téléphonique. En supposant l'authentification valide, l'équipement délivre l'information de validité de la communication au terminal qui gère alors la poursuite de la communication (bloc 17). Dès que la durée correspondant à la taxe prépayée est expirée, le dispositif en charge de cette fonction (par exemple, le terminal) déclenche une nouvelle perception

d'une taxe (bloc 15) par décrémentation du compteur d'unités prépayées de la carte.

On notera qu'entre l'établissement de la communication (bloc 14) et la fin de celle-ci, le terminal est en permanence en mesure de détecter une fin de communication. Cela est illustré en figure 2 par le bloc en pointillés 18 reliant les blocs 14 et 17. Une interruption de la communication peut, par exemple, être déclenchée par l'extraction de la carte du terminal.

On notera que l'organigramme de la figure 2 est extrêmement simplifié et a été représenté et décrit uniquement pour faire apparaître les procédures auxquelles s'applique plus particulièrement la présente invention, à savoir les procédures d'authentification.

La figure 3 représente, sous forme d'organigramme, les étapes principales d'une phase d'authentification, par un équipement de contrôle ou un dispositif d'authentification équivalent, d'une carte à puce de type téléphonique prépayée. L'organigramme de la figure 3 détaille les étapes des phases d'authentification mises en oeuvre aux blocs 13 et 13' de la figure 2.

Une phase d'authentification commence par la génération et l'envoi (la transmission), par le dispositif d'authentification, d'un nombre aléatoire NA (bloc 13-1) à destination de la carte. La carte met alors en oeuvre un algorithme de calcul prenant en compte, non seulement le nombre aléatoire NA reçu du dispositif d'authentification, mais également d'autres informations contenues dans la carte elle-même. Parmi ces informations, certaines sont des informations immuables de la carte et d'autres sont des informations variables. Les informations immuables comprennent, généralement, un identifiant de la carte (par exemple, son numéro de série NS), et une donnée secrète inscrite dans la carte directement lors de la fabrication et illisible par la suite (DS). Parmi les informations immuables, on peut également tenir compte de la valeur faciale (VF) de la carte prépayée, c'est-à-dire du nombre initial d'unités de compte qu'elle contient. Les informations variables prises en compte par

l'algorithme sont, notamment et entre autres, le nombre aléatoire NA ainsi que la valeur résiduelle VR de la carte, c'est-à-dire le nombre d'unités de compte non consommées. La mise en oeuvre de cet algorithme revient à effectuer le calcul d'un résultat R1 (bloc 13-2) fonction de l'ensemble de ces données. Le terminal lit (bloc 13-3) ce résultat R1 sur la carte et l'envoi au dispositif d'authentification, accompagné de toutes les données prises en compte pour son calcul à l'exception du nombre aléatoire NA et, généralement, de la donnée secrète DS. Cette donnée secrète DS est reconstituée (par exemple, lue dans une table) par le dispositif d'authentification à partir, au moins du numéro de série de la carte. La carte renvoie donc (le terminal les lit et les envoi) toutes les données du calcul effectué par la carte et qui sont inconnues du dispositif d'authentification.

A la figure 3, on a représenté par des blocs pointillés une variante qui sera décrite ultérieurement. Dans l'immédiat on ne tient compte que des blocs tracés en traits pleins.

A partir des informations R1, NS, VF et VR reçues de la carte, le dispositif d'authentification effectue une vérification de la cohérence du résultat par rapport aux données et notamment, par rapport au nombre aléatoire et de la donnée secrète qui ne lui a pas été retransmis par la carte. Ce calcul peut être illustré par le calcul d'un résultat R2 (bloc 13-4) prenant en compte les mêmes données que celles ayant servi au calcul, côté carte, du résultat R1. La donnée secrète est, par exemple, extraite d'une table de concordance à partir, par exemple, d'un identifiant de la carte (par exemple, son numéro de série). Une fois déterminée le résultat R2, le dispositif d'authentification compare ce résultat par rapport au résultat R1 que lui a communiqué le terminal (bloc 13-5). Si les deux résultats ne concordent pas, l'équipement contenant le dispositif d'authentification déclenche une coupure de la communication (bloc 13-6) qui est, soit mise en oeuvre directement soit communiquée au terminal. Si les deux résultats sont identiques, montrant que la carte est bien authentique, le dispositif d'authentification génère une

instruction de validation (bloc 13-7) à destination du terminal. Cette instruction correspond à celle communiquée pour l'établissement de la communication ou pour sa poursuite (bloc 14 ou 17, figure 2). Comme cela est représenté à la figure 3, l'instruction de coupure correspond généralement à la réponse du processus d'authentification adressée au terminal à la place de l'instruction de validation.

On notera que, pendant le processus d'authentification, le terminal n'intervient pas dans les échanges entre la carte et l'équipement de contrôle, sauf pour convertir les informations échangées au moyen de ses circuits d'interface. Toutefois, sa fonction de détection de fin de communication (bloc 18, figure 2) est bien entendu maintenue pendant les phases d'authentification.

Un procédé d'authentification tel que décrit en relation avec la figure 3 pose un problème de fiabilité en ce que le dispositif d'authentification ne peut pas être sûr que le débit enregistré sur la carte, c'est-à-dire le nombre d'unités prépayées consommées, correspond au débit côté équipement de contrôle. Ce problème est particulièrement sensible dans le domaine des communications téléphoniques où différents opérateurs se facturent des communications transitant par leurs réseaux respectifs. Dans un tel cas, la fiabilité du prépaiement doit concerner non seulement l'utilisateur final mais également la compensation entre opérateurs. La solution décrite ci-dessus résout les problèmes d'une éventuelle fraude par un utilisateur qui souhaiterait empêcher le débit de sa carte. Toutefois, elle n'est pas fiable vis-à-vis des opérateurs. En effet, à chaque fois qu'il émet un ordre de débit de taxe (bloc 15, figure 2), le central enregistre ce débit pour le refacturer ou le compenser auprès de l'opérateur ayant délivré (vendu) la carte à l'utilisateur. En supposant qu'une carte ayant servi à initialiser une communication dans un terminal soit sortie de ce terminal (sans détection d'erreur ou de fin de communication), par exemple avant débit, pour être introduite dans un terminal voisin et y être débitée d'une unité, cette carte une fois réintroduite dans le

premier terminal restera valablement authentifiée par l'équipement de contrôle qui attribuera une unité à l'opérateur alors que celle-ci n'aura pas été débitée à la carte par ce terminal. On peut considérer que l'incohérence entre la valeur résiduelle de la carte et les unités attribuées à l'opérateur correspond à un défaut d'authentification de la carte, car cela signifie une tentative de fraude.

Pour résoudre ce problème, la solution proposée aujourd'hui consiste à conserver, dans une mémoire vive de la carte, une donnée relative aux calculs. Cette solution est illustrée par les blocs pointillés de la figure 3. Selon cette solution, on mémorise, à l'issu de chaque calcul du résultat R1 de la carte, ce résultat (bloc 13-8 en pointillés). De plus, la valeur (R1(-1)) mémorisée lors de l'authentification précédente est prise en compte dans le calcul du résultat R1 courant (bloc 13-2). Côté équipement de contrôle, le calcul du résultat R2 (bloc 13-4) tient compte non seulement des paramètres décrits précédemment mais également du résultat R2(-1) mémorisé lors de l'authentification précédente. Cette mémorisation (bloc 13-9) s'effectue, par exemple, avant validation du résultat (bloc 13-7). En tenant compte du résultat de l'authentification précédente pour l'authentification courante, on peut ainsi s'assurer qu'une carte n'a pas subi un débit non pris en compte par l'équipement. Par conséquent, cette solution permet bien d'éviter une tentative de fraude par un opérateur indélicat qui chercherait à se voir créditer un nombre de taxes supérieur à celui que lui-même aurait débité aux utilisateurs.

Toutefois, les cartes actuelles utilisent pour la mise en oeuvre d'une telle solution un élément de mémoire vive (RAM) qui nécessite que la carte soit alimentée par le terminal pendant toute la communication pour préserver les valeurs mémorisées. Une telle alimentation permanente pose des problèmes de consommation au sein du terminal. Ceci est particulièrement gênant si le terminal dans lequel est introduit la carte n'est pas alimenté lui-même par une alimentation autonome ou par le secteur mais

reçoit son alimentation, par exemple, de la ligne téléphonique. On notera qu'en cas d'alimentation autonome au moyen de batteries, on cherche également à minimiser la consommation par le terminal. En prenant l'exemple d'un téléphone public à cartes prépayées, la consommation est classiquement comprise entre 1 et 5 milliampères pendant la phase d'authentification où la carte doit être alimentée pour le calcul, alors que la consommation globale du terminal doit rester inférieure à environ 16 à 20 milliampères. Parmi ces consommations, le simple maintien sous tension de la carte pour la mémorisation entraîne une consommation de l'ordre de 1 milliampère, ce qui est loin d'être négligeable.

La présente invention vise à proposer une nouvelle solution fiable pour l'authentification d'une carte à puce du type comprenant des unités de compte, ou analogues.

L'invention vise, plus particulièrement, à proposer un nouveau procédé d'authentification qui pallie les inconvénients des solutions connues.

L'invention vise également à proposer une solution qui minimise la consommation de la carte.

L'invention vise également à proposer une solution que ne nécessite aucune modification structurelle du terminal ni du dispositif d'authentification.

Pour atteindre ces objets, la présente invention prévoit un procédé d'authentification d'une carte à puce introduite dans un terminal propre à communiquer avec un dispositif d'authentification, comprenant les étapes suivantes :

génération d'un nombre aléatoire par le dispositif d'authentification ;

envoi de ce nombre aléatoire à la carte ;

calcul, par la carte, d'un premier résultat (R1) prenant en compte, entre autres, ledit nombre aléatoire et une valeur résiduelle d'unités de compte mémorisée dans la carte ;

envoi du premier résultat au dispositif d'authentification ;

calcul, par le dispositif d'authentification, d'un deuxième résultat prenant en compte les mêmes données que le premier résultat ; et

vérification, par le dispositif d'authentification, de la cohérence entre les deux résultats, le procédé consistant également à envoyer, de la carte au dispositif d'authentification, une donnée liée à la valeur résiduelle, et à mémoriser cette donnée dans le dispositif d'authentification.

Selon un mode de réalisation de la présente invention, le procédé est mis en oeuvre avant et après chaque changement de la valeur résiduelle de la carte.

Selon un mode de réalisation de la présente invention, on effectue, au sein du dispositif d'authentification, un test de cohérence de la donnée liée à la valeur résiduelle courante avec la donnée liée à la valeur résiduelle mémorisée lors de l'authentification précédente.

Selon un mode de réalisation de la présente invention, le test de cohérence consiste à vérifier l'identité entre lesdites données courante et précédente.

Selon un mode de réalisation de la présente invention, on utilise, entre autres, au moins une donnée immuable de la carte dans les calculs des deux résultats.

Selon un mode de réalisation de la présente invention, ladite donnée immuable n'est envoyée, de la carte au dispositif d'authentification, que lors d'une première authentification.

Selon un mode de réalisation de la présente invention, ladite donnée liée à la valeur résiduelle est la valeur résiduelle d'unités de compte elle-même.

La présente invention prévoit également un procédé de gestion des échanges entre une carte à puce et un terminal de commande en dépréciation de la valeur résiduelle en unités de compte stockées dans ladite carte.

Selon un mode de réalisation de la présente invention, ce procédé de gestion des échanges consiste :

à effectuer une authentification initiale lors de l'introduction de la carte dans le terminal en stockant, dans le dispositif d'authentification, des données intrinsèques immuables relatives à la carte ; et

à effectuer une phase d'authentification avant et après chaque besoin de dépréciation d'une unité de compte de la carte.

La présente invention prévoit en outre une carte à puce du type comprenant une zone de mémorisation d'unités de compte propres à être décomptées sur commande d'un terminal, et comprenant des moyens pour mettre en oeuvre le procédé d'authentification de l'invention.

Ces objets, caractéristiques et avantages, ainsi que d'autres de la présente invention seront exposés en détail dans la description suivante de modes de mise en oeuvre et de réalisation particuliers faite à titre non-limitatif en relation avec les figures jointes parmi lesquelles :

la figure 1 représente, de façon très schématique, un système à cartes à puce, du type auquel se rapporte la présente invention ;

la figure 2 représente, sous forme d'organigramme simplifié, un exemple classique d'étapes principales liées à l'authentification d'une carte prépayée lors d'une communication téléphonique ;

la figure 3 illustre, par un organigramme simplifié, deux procédés d'authentification classiques ;

la figure 4 représente, par un organigramme simplifié, les principales étapes d'une communication téléphonique au moyen d'une carte prépayée mettant en oeuvre la présente invention ;

la figure 5 est un organigramme plus détaillé d'une phase d'authentification initiale d'un mode de mise en oeuvre de la présente invention ; et

la figure 6 est un organigramme plus détaillé d'une phase répétitive d'authentification selon un mode de mise en oeuvre de la présente invention.

Les mêmes étapes ont été désignées par les mêmes références aux différentes figures. De plus, seules les étapes qui sont nécessaires à la compréhension de l'invention ont été représentées aux figures et seront décrites par la suite. En particulier, on ne mettra l'accent que sur les étapes liées à l'authentification de la carte à puce sans se préoccuper des autres étapes nécessaires à l'établissement et au bon déroulement de la communication téléphonique prise pour exemple. En particulier, on notera que les échanges d'informations entre le terminal et l'équipement de contrôle s'effectuent, s'ils transitent sur les lignes téléphoniques, généralement en utilisant des fréquences supravocales.

Une caractéristique de la présente invention est de stocker, dans le dispositif d'authentification, au moins une donnée liée à la valeur résiduelle de la carte à puce introduite dans le terminal. Ainsi, selon la présente invention, on prévoit d'envoyer, à chaque authentification, la valeur résiduelle de la carte (ou une donnée liée) pour que celle-ci soit stockée par le dispositif d'authentification de l'équipement de contrôle. Cela lui permet de comparer cette valeur résiduelle mémorisée par rapport à la valeur résiduelle qui lui est envoyée à l'authentification suivante et, par conséquent, de vérifier que les deux valeurs sont cohérentes entre elles, ce qui garantit que la carte n'a pas été modifiée entre les deux authentifications, c'est-à-dire qu'elle n'a pas subi de débit hors du terminal ou été utilisée par un autre terminal.

Une autre caractéristique d'un mode de réalisation préféré de l'invention est que les autres données propres à la carte qui sont utilisées par le dispositif d'authentification pour mettre en oeuvre le même algorithme que celui mis en oeuvre au sein de la carte, sont stockées dans le dispositif d'authentification lors de l'initialisation de la communication. Plus précisément, on mémorise ces données au cours d'une première phase d'authentification. Ces données concernent plus particulièrement les informations dites permanentes ou immuables de la

carte à savoir, par exemple, son numéro de série, sa valeur faciale et autres informations fixes. Un avantage est alors que l'on minimise les besoins d'échange d'information entre la carte et l'équipement pour les autres authentifications.

Une autre caractéristique de l'invention est de prévoir une phase d'authentification avant et après chaque ordre de décompte d'une unité par le terminal à destination de la carte. Ainsi, en cours de communication, l'invention double de nombre de phases d'authentification par rapport aux procédés classiques. Toutefois, ce qui paraît à première vue être un inconvénient eu égard au volume d'informations à transmettre dans la bande de fréquences supravocales qui est connue pour n'autoriser qu'un débit limité, s'avère en fait être un avantage. En effet, le nombre d'informations transmises à chaque phase d'authentification, de la carte au dispositif d'authentification, est limité. Par conséquent, les durées nécessaires aux transmissions d'informations sont réduites par rapport aux procédés classiques, ce qui rend possible d'effectuer des phases d'authentification supplémentaires. Or ces phases supplémentaires optimisent la sécurité des transactions.

La figure 4 représente un organigramme simplifié d'un mode de mise en oeuvre de la présente invention. La figure 4 est à rapprocher de la figure 2 décrite précédemment et dont l'invention reprend les étapes (10 d'introduction de la carte, 11 de détection par le terminal et 12 de connexion au dispositif d'authentification) jusqu'à la première phase d'authentification.

Selon la présente invention, la première phase d'authentification A (bloc 21, figure 4) est différente des autres authentifications de la communication.

Cette phase initiale d'authentification de l'invention est décrite selon un mode de mise en oeuvre préféré en relation avec la figure 5. On commence, comme dans une authentification classique (figure 3), par procéder à l'envoi d'un nombre aléatoire NA par le central à destination de la carte (bloc 13-1). Côté carte, on calcule comme précédemment un résultat d'appli-

cation d'un algorithme (bloc 13-2). Ce résultat R1 est fonction, par exemple, du numéro de série NS, d'une donnée secrète DS, de la valeur faciale VF, de la valeur résiduelle VR et du nombre aléatoire NA. Selon l'invention, aucune valeur n'a besoin d'être mémorisée dans la carte à l'exception bien entendu de la valeur résiduelle par décrémentation du compteur agissant, par exemple, sur une mémoire morte par exemple de type EPROM ou EEPROM. La carte renvoie (bloc 13-3), à destination du dispositif d'authentification, le résultat R1 de son calcul ainsi que, dans cette phase initiale d'authentification, les informations NS, VF, et VR ayant servi au calcul.

Selon l'invention, les données immuables de la carte sont mémorisées (bloc 22) par le dispositif d'authentification. Il s'agit, dans cet exemple, du numéro de série NS et de la valeur faciale VF (ou de données liées à ces informations), et de la donnée secrète DS, cette dernière étant récupérée, côté équipement, à partir par exemple du numéro de série. De plus, on mémorise également la valeur résiduelle VR de la carte.

On procède alors, de façon classique, au calcul d'un résultat R2 par la mise en oeuvre d'un algorithme équivalent à celui mis en oeuvre par la carte (bloc 13-4). Puis, on vérifie la concordance des deux résultats R1 et R2 (bloc 13-5). Enfin, le résultat de cette comparaison est interprété par l'équipement pour provoquer, soit la coupure (bloc 13-6), soit la validation (bloc 13-7) de la communication. On notera que, selon l'invention, le résultat R2 n'a pas besoin d'être mémorisé par l'équipement.

En reprenant l'organigramme de la figure 4, et en supposant une validation de la carte authentifiée dans la phase 21, la communication peut s'établir de manière classique (bloc 14). Cet établissement doit être suivi d'un premier débit d'une unité prépayée sur la carte.

Selon l'invention, l'ordre de débit (bloc 15) d'une unité par le central est précédé d'une phase d'authentification B (bloc 23) d'un deuxième type. Cette phase d'authentification doit

valider ou invalider la poursuite de la communication avant même le prélèvement de la taxe, pour s'assurer que la carte n'a pas été modifiée depuis la précédente authentification.

Un exemple de phase d'authentification 23 est détaillé par l'organigramme de la figure 6. Les deux premières étapes d'envoi d'un nombre aléatoire 13-1 et de mise en oeuvre de l'algorithme de détermination du résultat R1 par la carte 13-2 restent classiques. Toutefois, selon l'invention, la carte n'envoie plus désormais, à destination de l'équipement, que le résultat R1 ainsi que sa valeur résiduelle VR (bloc 24). Dans la phase d'authentification B précédant le prélèvement d'une taxe, l'équipement mémorise également (bloc 25) la valeur résiduelle qui est ici inchangée par rapport à la valeur précédente. Puis, on met en oeuvre l'algorithme de calcul du résultat R2 de façon classique (bloc 13-4).

Selon l'invention, ce calcul est suivi de deux contrôles de la carte. Un premier contrôle (bloc 13-5) correspond à la comparaison classique des résultats R2 et R1. Si les résultats ne concordent pas, on passe à l'étape de coupure classique (13-6) de la communication. Toutefois, si les résultats concordent, l'équipement effectue une deuxième vérification (bloc 26) qui consiste à comparer la valeur résiduelle courante VRc qu'il vient de recevoir à la valeur résiduelle VRp mémorisée lors de l'authentification précédente. Quand il s'agit de la première étape de prélèvement de taxe de la communication, cette valeur VR correspond à la valeur résiduelle mémorisée lors de l'authentification A (bloc 21). Si les deux valeurs résiduelles ne concordent pas, cela signifie un défaut d'authenticité de la carte. Par exemple, il peut s'agir d'une carte qui a été sortie du terminal puis réintroduite dans un autre dans lequel elle a subi un débit d'une unité sans que celui-ci soit pris en compte par l'équipement de contrôle. Dans ce cas, l'équipement provoque la coupure (bloc 13-6) de la communication. Si les deux valeurs résiduelles concordent, l'équipement valide (bloc 13-7) la communication de façon classique. Cette validation est illustrée en

figure 4 par un bloc 17-1 d'indication de poursuite de communication. L'authentification 23 est alors suivie d'un ordre de débit de taxe classique 15 qui est communiqué à la carte comme dans un procédé classique. Le compteur de valeur résiduelle de la carte est alors décrémentée de façon classique (bloc 16).

Puis, selon l'invention, on met en oeuvre une phase d'authentification C (bloc 27) qui a pour objet, notamment, de mémoriser la nouvelle valeur résiduelle de la carte au sein du dispositif d'authentification. La phase d'authentification 27 reprend les étapes illustrées par la figure 6 à l'exception, le cas échéant, du test 26 sur la valeur résiduelle. La mémorisation de la nouvelle valeur VR permettra ultérieurement au dispositif d'authentification de valider la communication avant le débit d'une autre unité. Si l'authentification C est acceptée, la communication se poursuit (bloc 17-2, figure 4) et on revient en attente d'un nouveau besoin de débit d'unité.

A titre de variante, on pourra maintenir le test sur la valeur résiduelle mais en comparant la valeur courante VRc à la valeur précédente moins 1, Vrp-1.

Selon l'invention, avant chaque débit, on met en oeuvre une phase d'authentification de type B, et chaque débit est suivi d'une phase d'authentification de type C.

Un avantage de la présente invention est qu'en prévoyant des phases d'authentification avant et après chaque débit d'unité, on améliore la fiabilité du système. On notera que le choix de vérifier la valeur résiduelle au moins avant le débit permet d'éviter tout défaut de perception, même d'une seule taxe.

Un autre avantage de l'invention est que cette amélioration s'effectue sans aucune modification structurelle des terminaux (lecteurs de carte) ou des dispositifs d'authentification. En effet, ces derniers font le plus souvent appel à des systèmes informatiques de traitement. Il suffit alors de modifier le programme de traitement pour l'adapter aux trois phases d'authentification de l'invention.

Un autre avantage de l'invention est que la mise en oeuvre du procédé d'authentification trouve un intérêt non seulement au sein d'un dispositif distant, par l'intermédiaire de la liaison téléphonique, mais également quand ce procédé est mis en oeuvre par le terminal lui-même. Dans le premier cas, on réduit la durée de la communication qui est nécessaire pour l'échange d'informations en bande supravocale, en particulier, lorsque les communications sont relativement longues en entraînent plusieurs débits d'unités. En effet, on tire alors pleinement profit de ne transmettre, à chaque authentification postérieure à la première, uniquement la valeur résiduelle VR et le résultat R1. Dans le deuxième cas, où le dispositif d'authentification est intégré au terminal, on minimise la consommation en limitant les périodes d'alimentation de la carte aux phases d'authentification.

Ce dernier avantage est également important dans le cas où le terminal d'introduction de la carte est dépourvu d'alimentation propre et tire son énergie de la ligne téléphonique.

Bien entendu, la présente invention est susceptible de diverses variantes et modifications qui apparaîtront à l'homme de l'art. En particulier, d'autres informations immuables ou variables que celles prisent pour exemple dans la description qui précède pourront être utilisées.

De plus, on notera que toutes les informations relatives à la carte ne sont pas nécessairement accessibles directement sous forme de numéro mais peuvent correspondre à des combinaisons binaires représentant une donnée fonction de ces informations. En particulier, on pourra prévoir de ne transmettre, à chaque phase d'authentification, que le résultat R1 de l'algorithme et de mémoriser sa valeur, côté dispositif d'authentification. Le deuxième test (26) compare alors les valeurs courante et précédente du résultat R1. Toutefois, l'envoi d'une donnée individuelle liée à la valeur résiduelle améliore encore la fiabilité de l'authentification.

En outre, les étapes d'authentification décrites dans l'exemple de mise en oeuvre du procédé de l'invention pourront

être effectuées dans un autre ordre pourvu de respecter les indications fonctionnelles données ci-dessus. En particulier, le test de cohérence de la valeur résiduelle de la carte pourra être effectué avant le test de cohérence des résultats d'algorithme, voire avant même le calcul de l'algorithme par le dispositif d'authentification. Enfin, bien que l'invention ait été décrite ci-dessus en relation avec un exemple d'application aux communications téléphoniques au moyen de cartes prépayées, on notera que l'invention s'applique plus généralement à tout système utilisant une carte à puce pourvue d'un compteur décrémentant des unités mémorisées.

## REVENDICATIONS

1. Procédé d'authentification (A, B, C) d'une carte (3) à puce (4) introduite dans un terminal (1) propre à communiquer avec un dispositif d'authentification (2), comprenant les étapes suivantes :

génération d'un nombre aléatoire (NA) par le dispositif d'authentification (2) ;

envoi (13-1) de ce nombre aléatoire à la carte ;

calcul (13-2), par la carte, d'un premier résultat (R1) prenant en compte, entre autres, ledit nombre aléatoire et une valeur résiduelle (VR) d'unités de compte mémorisée dans la carte ;

envoi (13-3, 24) du premier résultat au dispositif d'authentification ;

calcul (13-4), par le dispositif d'authentification, d'un deuxième résultat (R2) prenant en compte les mêmes données que le premier résultat ; et

vérification (13-5), par le dispositif d'authentification, de la cohérence entre les deux résultats,

caractérisé en ce qu'il consiste :

à envoyer (13-3, 24), de la carte au dispositif d'authentification, une donnée liée à la valeur résiduelle ;

à mémoriser (22, 25) cette donnée dans le dispositif d'authentification ; et

à effectuer, au sein du dispositif d'authentification (2), un test (26) de cohérence de la donnée liée à la valeur résiduelle courante (VRc) avec la donnée liée à la valeur résiduelle (VRp) mémorisée lors de l'authentification précédente.

2. Procédé d'authentification selon la revendication 1, caractérisé en ce qu'il est mis en oeuvre avant et après chaque changement (16) de la valeur résiduelle de la carte (3).

3. Procédé d'authentification selon la revendication 1 ou 2, caractérisé en ce que le test de cohérence (26) consiste à vérifier l'identité entre lesdites données courante (VRc) et précédente (VRp).

4. Procédé d'authentification selon l'une quelconque des revendications 1 à 3, caractérisé en ce qu'il consiste à utiliser, entre autres, au moins une donnée immuable (VF, NS, DS) de la carte (3) dans les calculs des deux résultats (R1, R2).

5. Procédé d'authentification selon la revendication 4, caractérisé en ce que ladite donnée immuable (VF, NS) n'est envoyée (13-3), de la carte (3) au dispositif d'authentification (2), que lors d'une première authentification (A).

6. Procédé d'authentification selon l'une quelconque des revendications 1 à 5, caractérisé en ce que ladite donnée liée à la valeur résiduelle est la valeur résiduelle (VR) d'unités de compte elle-même.

7. Procédé de gestion des échanges entre une carte (3) à puce (4) et un terminal (2) de commande en dépréciation de la valeur résiduelle (VR) en unités de compte stockées dans ladite carte, caractérisé en ce qu'il consiste à mettre en oeuvre le procédé d'authentification selon l'une quelconque des revendications 1 à 6.

8. Procédé selon la revendication 7, caractérisé en ce qu'il consiste :

à effectuer une authentification initiale (A) lors de l'introduction de la carte (3) dans le terminal (1) en stockant, dans le dispositif d'authentification (2), des données intrinsèques immuables (VF, DS, NS) relatives à la carte ; et

à effectuer une phase d'authentification avant (B) et après (C) chaque besoin de dépréciation d'une unité de compte de la carte.

9. Carte à puce du type comprenant une zone de mémorisation d'unités de compte propres à être décomptées sur commande d'un terminal, caractérisée en ce qu'elle comporte des moyens pour mettre en oeuvre le procédé d'authentification selon l'une quelconque des revendications 1 à 8.

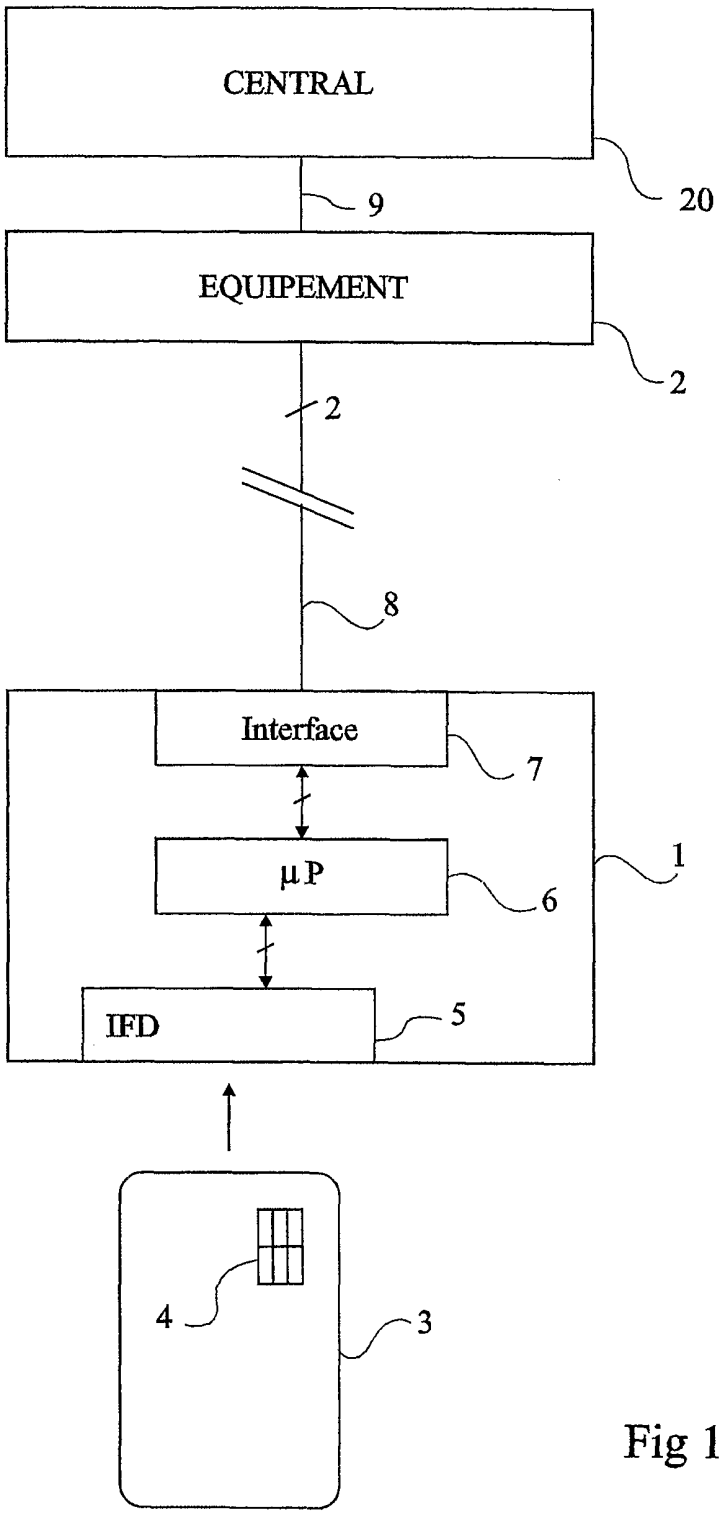


Fig 1

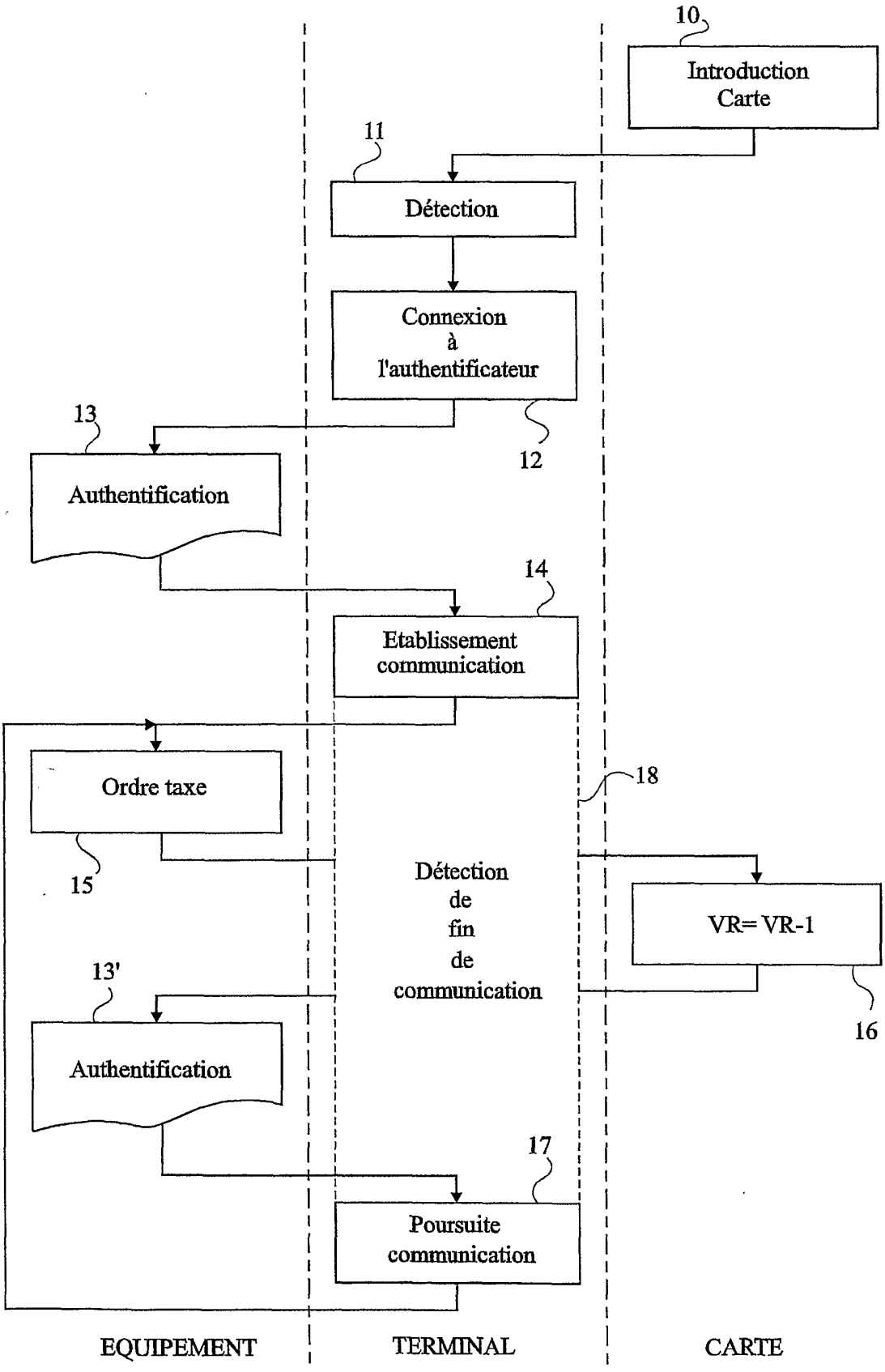
10
Introduction Carte
11
Détection
Connexion à l'authentificateur
12
13
Authentification
14
Etablissement communication
Ordre taxe
15
18
Détection de fin de communication
VR= VR-1
16
13'
Authentification
17
Poursuite communication
EQUIPEMENT
TERMINAL
CARTE

Fig 2

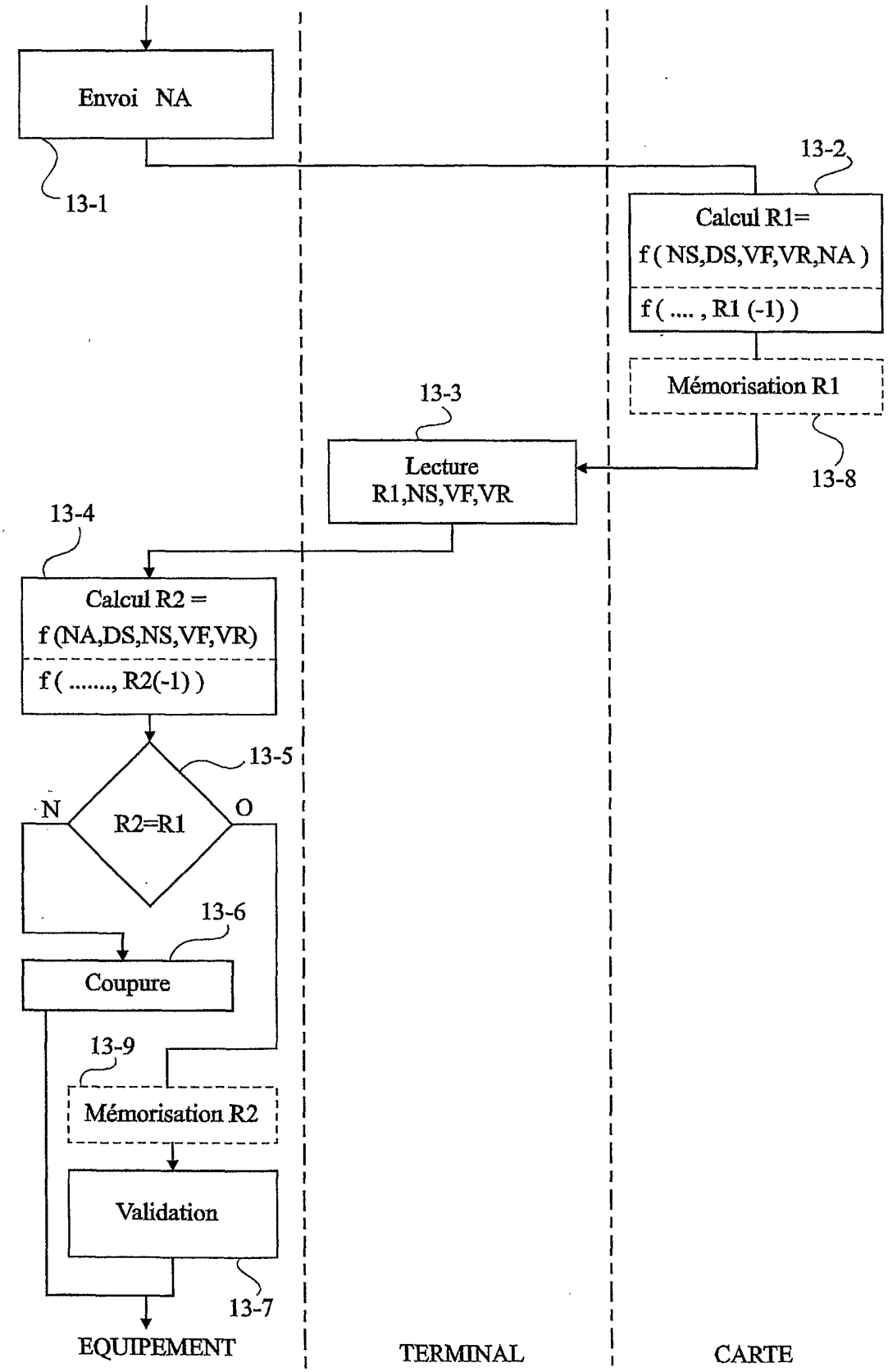
Envoi NA
13-1
13-2
Calcul R1=
f ( NS,DS,VF,VR,NA )
f ( .... , R1 (-1) )
Mémorisation R1
13-8
13-3
Lecture
R1,NS,VF,VR
13-4
Calcul R2 =
f (NA,DS,NS,VF,VR)
f ( ....., R2(-1) )
13-5
N
R2=R1
O
13-6
Coupure
13-9
Mémorisation R2
Validation
13-7
EQUIPEMENT
TERMINAL
CARTE

Fig 3

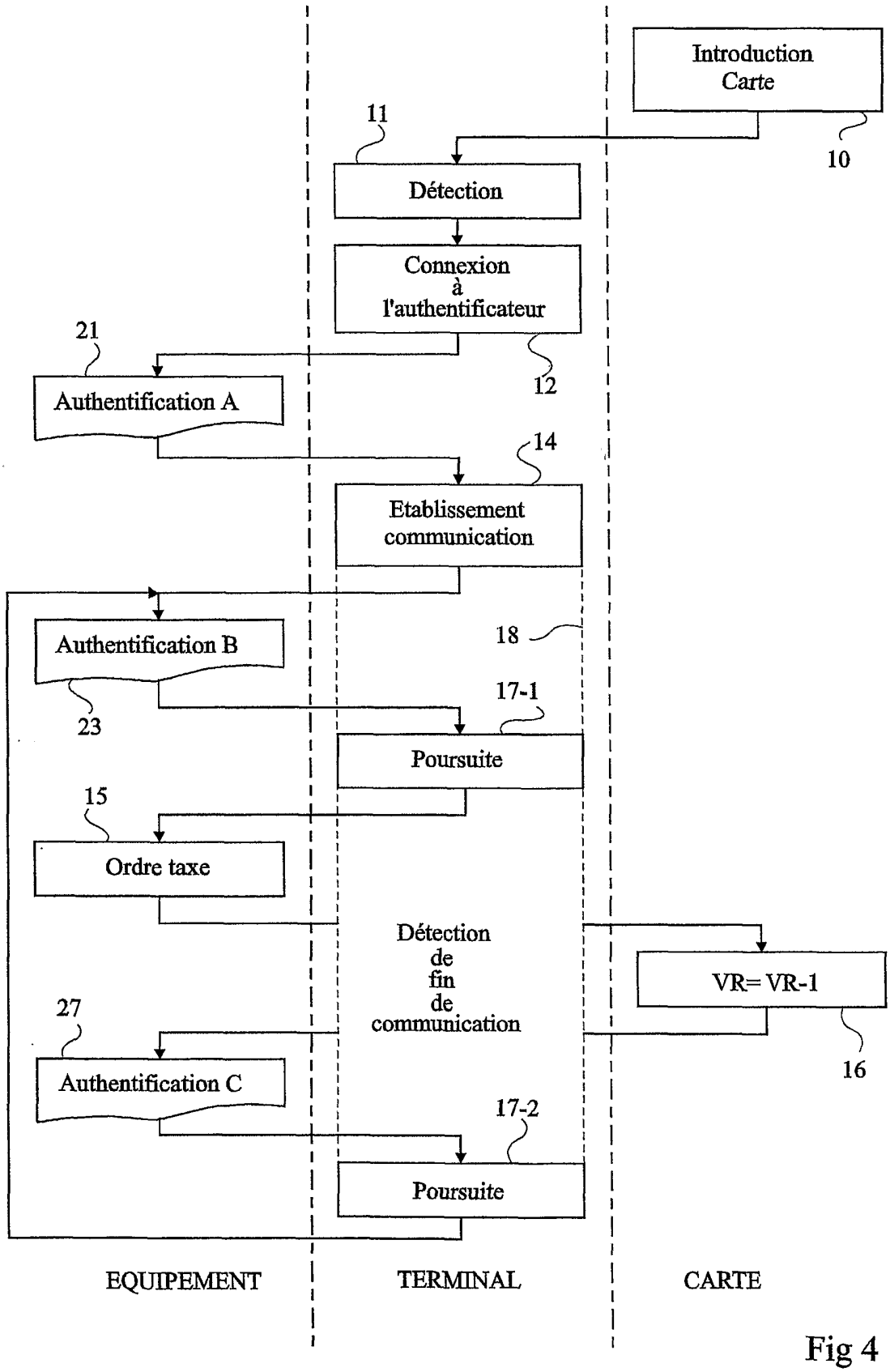
Introduction Carte
10
11
Détection
Connexion à l'authentificateur
12
21
Authentification A
14
Etablissement communication
18
Authentification B
23
17-1
Poursuite
15
Ordre taxe
Détection de fin de communication
VR= VR-1
16
27
Authentification C
17-2
Poursuite
EQUIPEMENT
TERMINAL
CARTE

Fig 4

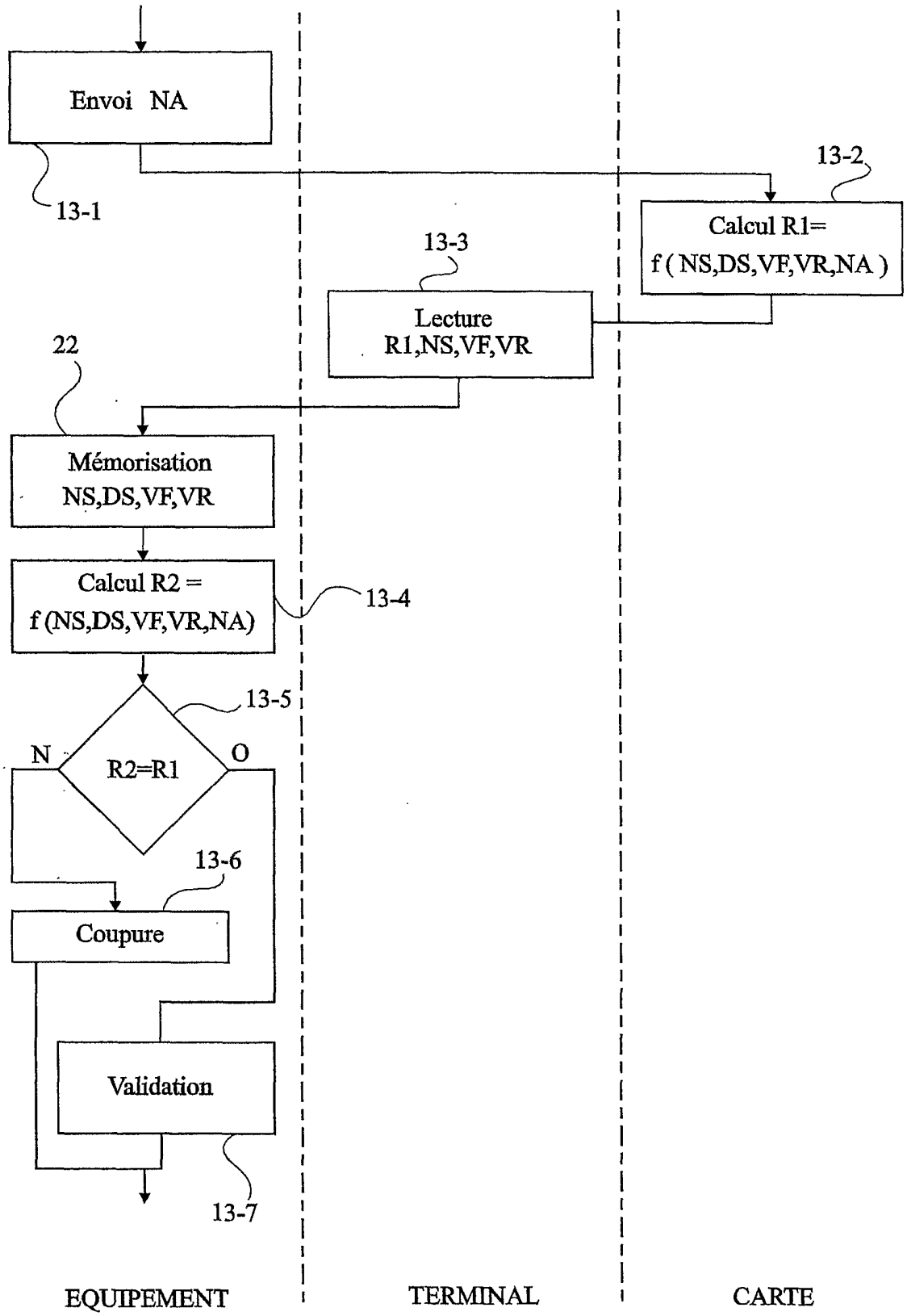
Envoi NA
13-1
13-2
Calcul R1=
f ( NS,DS,VF,VR,NA )
13-3
Lecture
R1,NS,VF,VR
22
Mémorisation
NS,DS,VF,VR
Calcul R2 =
f (NS,DS,VF,VR,NA)
13-4
13-5
N
R2=R1
O
13-6
Coupure
Validation
13-7
EQUIPEMENT
TERMINAL
CARTE

Fig 5

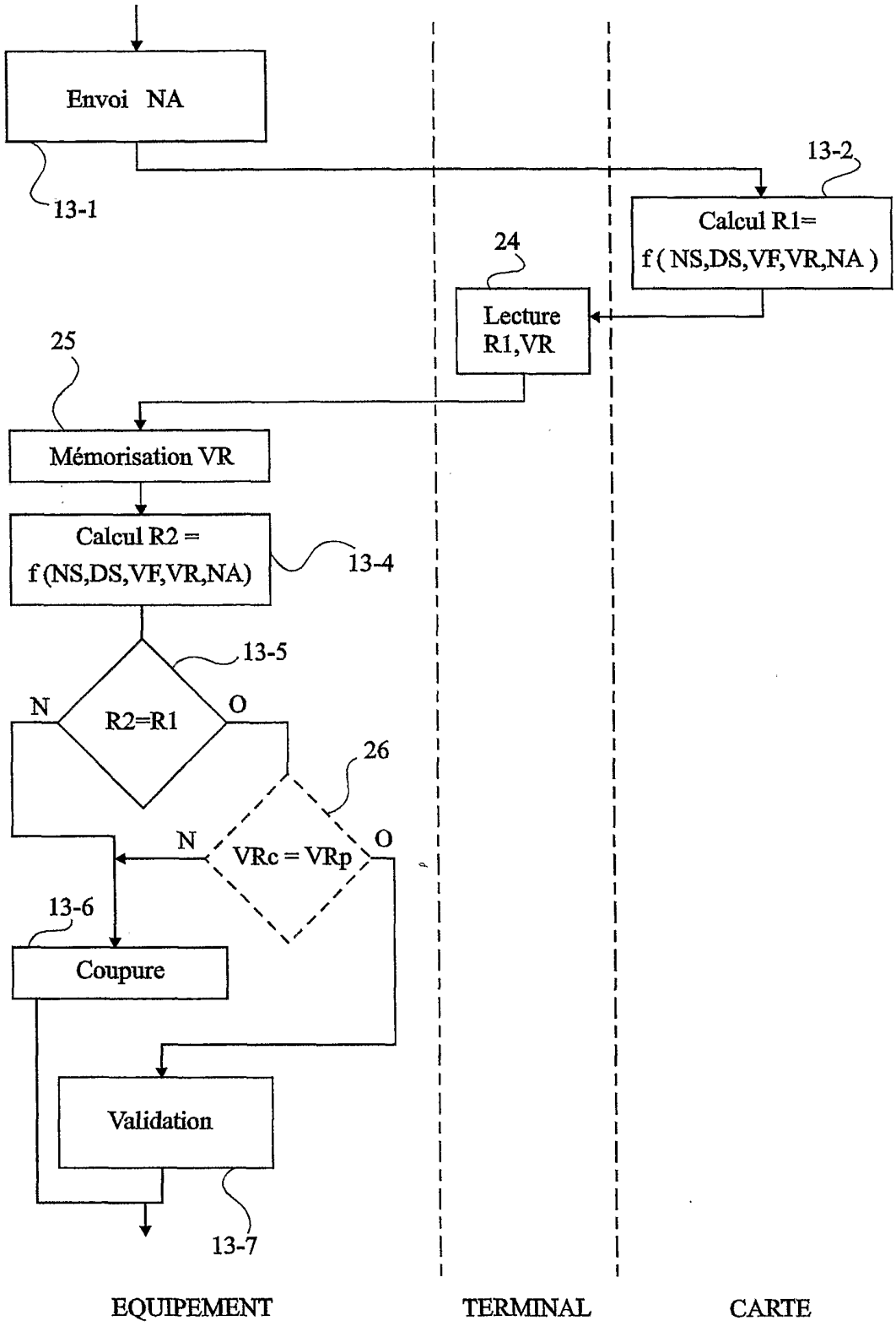
Envoi NA
13-1
13-2
Calcul R1=
f ( NS,DS,VF,VR,NA )
24
Lecture
R1,VR
25
Mémorisation VR
Calcul R2 =
f (NS,DS,VF,VR,NA)
13-4
13-5
N
R2=R1
O
26
N
VRc = VRp
O
13-6
Coupure
Validation
13-7
EQUIPEMENT
TERMINAL
CARTE

Fig 6

# INTERNATIONAL SEARCH REPORT

ernational Application No
PCT/FR 01/00955

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | WO 97 22091 A (KONINKLIJKE PTT NEDERLAND)<br>19 June 1997 (1997-06-19)<br>abstract; claims; figures | 1,2,4-9 |
| A | EP 0 574 990 A (PHILIPS PATENTVERWALTUNG)<br>22 December 1993 (1993-12-22)<br>abstract; claims; figures | 1,2,6,7,<br>9 |
| A | EP 0 570 924 A (SIEMENS)<br>24 November 1993 (1993-11-24)<br>abstract; claims; figure | 1,4,6,7,<br>9 |
| A | WO 97 21198 A (LANDIS & GYR)<br>12 June 1997 (1997-06-12)<br>abstract; claims; figures | 1,2,4,<br>6-9 |

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 10 July 2001 | 17/07/2001 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL – 2280 HV Rijswijk<br>Tel. (+31–70) 340–2040, Tx. 31 651 epo nl,<br>Fax: (+31–70) 340–3016 | David, J |

1

Form PCT/ISA/210 (second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

ernational Application No
PCT/FR 01/00955

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication,where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | EP 0 621 570 A (FRANCE TELECOM)<br>26 October 1994 (1994-10-26)<br>the whole document | 1,2,4-9 |
| A | EP 0 637 004 A (KONINKLIJKE PTT NEDERLAND)<br>1 February 1995 (1995-02-01)<br>the whole document | 1-3,7-9 |
| A | WO 97 22093 A (LANDIS & GYR)<br>19 June 1997 (1997-06-19) | |
| A | WO 97 21197 A (LANDIS & GYR)<br>12 June 1997 (1997-06-12) | |

1

# INTERNATIONAL SEARCH REPORT

Information on patent family members

ernational Application No
PCT/FR 01/00955

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| WO 9722091 A | 19-06-1997 | NL 1001863 C | 10-06-1997 |
| | | AT 190420 T | 15-03-2000 |
| | | AU 703985 B | 01-04-1999 |
| | | AU 7625496 A | 03-07-1997 |
| | | BG 102607 A | 29-01-1999 |
| | | BR 9611975 A | 17-02-1999 |
| | | CA 2239875 A | 19-06-1997 |
| | | CN 1203681 A | 30-12-1998 |
| | | CZ 9801758 A | 13-01-1999 |
| | | DE 69607041 D | 13-04-2000 |
| | | DE 69607041 T | 13-07-2000 |
| | | EP 0883866 A | 16-12-1998 |
| | | ES 2143790 T | 16-05-2000 |
| | | NO 982527 A | 03-06-1998 |
| | | NZ 322489 A | 28-10-1998 |
| | | PL 327192 A | 23-11-1998 |
| | | US 5991412 A | 23-11-1999 |
| EP 0574990 A | 22-12-1993 | DE 4219739 A | 23-12-1993 |
| | | DE 59309320 D | 04-03-1999 |
| | | JP 6215208 A | 05-08-1994 |
| | | US 5436971 A | 25-07-1995 |
| EP 0570924 A | 24-11-1993 | DE 59308837 D | 10-09-1998 |
| | | DK 570828 T | 10-05-1999 |
| | | EP 0570828 A | 24-11-1993 |
| | | ES 2119832 T | 16-10-1998 |
| WO 9721198 A | 12-06-1997 | CH 689813 A | 30-11-1999 |
| | | AU 716546 B | 24-02-2000 |
| | | AU 1096497 A | 27-06-1997 |
| | | DE 59602905 D | 30-09-1999 |
| | | EP 0865643 A | 23-09-1998 |
| EP 0621570 A | 26-10-1994 | FR 2704081 A | 21-10-1994 |
| | | DE 69407647 D | 12-02-1998 |
| | | DE 69407647 T | 09-07-1998 |
| | | JP 7110876 A | 25-04-1995 |
| | | US 5495098 A | 27-02-1996 |
| EP 0637004 A | 01-02-1995 | NL 9301271 A | 16-02-1995 |
| | | AT 158432 T | 15-10-1997 |
| | | CA 2128355 A | 21-01-1995 |
| | | DE 69405664 D | 23-10-1997 |
| | | DE 69405664 T | 19-03-1998 |
| | | DK 637004 T | 14-04-1998 |
| | | EP 0775991 A | 28-05-1997 |
| | | ES 2107090 T | 16-11-1997 |
| | | GR 3025686 T | 31-03-1998 |
| | | US 5914471 A | 22-06-1999 |
| WO 9722093 A | 19-06-1997 | CH 690530 A | 29-09-2000 |
| | | AU 704773 B | 06-05-1999 |
| | | AU 1140497 A | 03-07-1997 |
| | | EP 0870286 A | 14-10-1998 |
| WO 9721197 A | 12-06-1997 | CH 689812 A | 30-11-1999 |
| | | AU 703043 B | 11-03-1999 |

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR 01/00955

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| WO 9721197 A | | AU 1094297 A | 27-06-1997 |
| | | DE 59601908 D | 17-06-1999 |
| | | EP 0864138 A | 16-09-1998 |

# RAPPORT DE RECHERCHE INTERNATIONALE

nande Internationale No
PCT/FR 01/00955

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G07F7/08

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

| Catégorie ° | Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents | no. des revendications visées |
|---|---|---|
| A | WO 97 22091 A (KONINKLIJKE PTT NEDERLAND)<br>19 juin 1997 (1997-06-19)<br>abrégé; revendications; figures | 1,2,4-9 |
| A | EP 0 574 990 A (PHILIPS PATENTVERWALTUNG)<br>22 décembre 1993 (1993-12-22)<br>abrégé; revendications; figures | 1,2,6,7,<br>9 |
| A | EP 0 570 924 A (SIEMENS)<br>24 novembre 1993 (1993-11-24)<br>abrégé; revendications; figure | 1,4,6,7,<br>9 |
| A | WO 97 21198 A (LANDIS & GYR)<br>12 juin 1997 (1997-06-12)<br>abrégé; revendications; figures | 1,2,4,<br>6-9 |

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

| Date à laquelle la recherche internationale a été effectivement achevée | Date d'expédition du présent rapport de recherche internationale |
|---|---|
| 10 juillet 2001 | 17/07/2001 |

| Nom et adresse postale de l'administration chargée de la recherche internationale | Fonctionnaire autorisé |
|---|---|
| Office Européen des Brevets, P.B. 5818 Patentlaan 2<br>NL – 2280 HV Rijswijk<br>Tel. (+31–70) 340–2040, Tx. 31 651 epo nl,<br>Fax: (+31–70) 340–3016 | David, J |

1

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

# RAPPORT DE RECHERCHE INTERNATIONALE

mande Internationale No
PCT/FR 01/00955

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

| Catégorie ° | Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents | no. des revendications visées |
|---|---|---|
| X | EP 0 621 570 A (FRANCE TELECOM)<br>26 octobre 1994 (1994-10-26)<br>le document en entier | 1,2,4-9 |
| A | EP 0 637 004 A (KONINKLIJKE PTT NEDERLAND)<br>1 février 1995 (1995-02-01)<br>le document en entier | 1-3,7-9 |
| A | WO 97 22093 A (LANDIS & GYR)<br>19 juin 1997 (1997-06-19) | |
| A | WO 97 21197 A (LANDIS & GYR)<br>12 juin 1997 (1997-06-12) | |

1

# RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

mande Internationale No
PCT/FR 01/00955

| Document brevet cité au rapport de recherche | Date de publication | Membre(s) de la famille de brevet(s) | Date de publication |
|---|---|---|---|
| WO 9722091 A | 19-06-1997 | NL 1001863 C | 10-06-1997 |
| | | AT 190420 T | 15-03-2000 |
| | | AU 703985 B | 01-04-1999 |
| | | AU 7625496 A | 03-07-1997 |
| | | BG 102607 A | 29-01-1999 |
| | | BR 9611975 A | 17-02-1999 |
| | | CA 2239875 A | 19-06-1997 |
| | | CN 1203681 A | 30-12-1998 |
| | | CZ 9801758 A | 13-01-1999 |
| | | DE 69607041 D | 13-04-2000 |
| | | DE 69607041 T | 13-07-2000 |
| | | EP 0883866 A | 16-12-1998 |
| | | ES 2143790 T | 16-05-2000 |
| | | NO 982527 A | 03-06-1998 |
| | | NZ 322489 A | 28-10-1998 |
| | | PL 327192 A | 23-11-1998 |
| | | US 5991412 A | 23-11-1999 |
| EP 0574990 A | 22-12-1993 | DE 4219739 A | 23-12-1993 |
| | | DE 59309320 D | 04-03-1999 |
| | | JP 6215208 A | 05-08-1994 |
| | | US 5436971 A | 25-07-1995 |
| EP 0570924 A | 24-11-1993 | DE 59308837 D | 10-09-1998 |
| | | DK 570828 T | 10-05-1999 |
| | | EP 0570828 A | 24-11-1993 |
| | | ES 2119832 T | 16-10-1998 |
| WO 9721198 A | 12-06-1997 | CH 689813 A | 30-11-1999 |
| | | AU 716546 B | 24-02-2000 |
| | | AU 1096497 A | 27-06-1997 |
| | | DE 59602905 D | 30-09-1999 |
| | | EP 0865643 A | 23-09-1998 |
| EP 0621570 A | 26-10-1994 | FR 2704081 A | 21-10-1994 |
| | | DE 69407647 D | 12-02-1998 |
| | | DE 69407647 T | 09-07-1998 |
| | | JP 7110876 A | 25-04-1995 |
| | | US 5495098 A | 27-02-1996 |
| EP 0637004 A | 01-02-1995 | NL 9301271 A | 16-02-1995 |
| | | AT 158432 T | 15-10-1997 |
| | | CA 2128355 A | 21-01-1995 |
| | | DE 69405664 D | 23-10-1997 |
| | | DE 69405664 T | 19-03-1998 |
| | | DK 637004 T | 14-04-1998 |
| | | EP 0775991 A | 28-05-1997 |
| | | ES 2107090 T | 16-11-1997 |
| | | GR 3025686 T | 31-03-1998 |
| | | US 5914471 A | 22-06-1999 |
| WO 9722093 A | 19-06-1997 | CH 690530 A | 29-09-2000 |
| | | AU 704773 B | 06-05-1999 |
| | | AU 1140497 A | 03-07-1997 |
| | | EP 0870286 A | 14-10-1998 |
| WO 9721197 A | 12-06-1997 | CH 689812 A | 30-11-1999 |
| | | AU 703043 B | 11-03-1999 |

# RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

nande Internationale No
PCT/FR 01/00955

| Document brevet cité au rapport de recherche | Date de publication | Membre(s) de la famille de brevet(s) | Date de publication |
|---|---|---|---|
| WO 9721197 A | | AU 1094297 A | 27-06-1997 |
| | | DE 59601908 D | 17-06-1999 |
| | | EP 0864138 A | 16-09-1998 |