(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Numéro de publication: **0 413 636 A1**

(12) DEMANDE DE BREVET EUROPEEN

(21) Numéro de dépôt: **90402298.5**

(22) Date de dépôt: **16.08.90**

(51) Int. Cl.5: **G07F 9/06**, G07F 17/24, G07B 15/00

(30) Priorité: **17.08.89 FR 8910962**

(43) Date de publication de la demande: **20.02.91 Bulletin 91/08**

(84) Etats contractants désignés: **DE ES GB IT NL**

(71) Demandeur: **SCHLUMBERGER INDUSTRIES**
50, avenue Jean Jaurès
F-92120 Montrouge(FR)

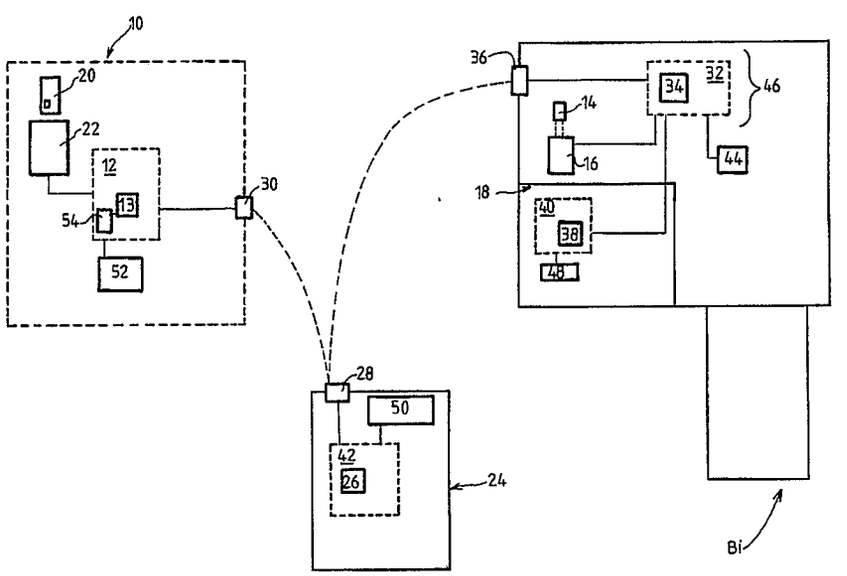
(72) Inventeur: **Lelouch, Franck**
70, quai du Petit Parc
F-94100 Saint-Maur(FR)
Inventeur: **Ferrus, Joelle**
11, chemin des Relançons
F-25000 Besançon(FR)

(74) Mandataire: **Dronne, Guy et al**
Cabinet BEAU de LOMENIE, 55, rue d'Amsterdam
F-75008 Paris(FR)

(54) Système et procédé pour contrôler la collecte de bornes à prépaiement.

(57) La présente invention a pour objet un système et un procédé pour sécuriser et contrôler la collecte de bornes à prépaiement notamment de bornes de stationnement payant pour véhicules.

Le système comprend un centre de collecte (10), des bornes (B_1...B_i) comprenant chacune un coffre (18) pour le stockage temporaire des pièces de monnaie introduites dans ladite borne et des moyens de mémorisation (34, 38) pour mémoriser des informations spécifiques à chaque borne B_i,des moyens de dialogue (24, 28, 30, 36) entre ledit centre de collecte (10) et lesdites bornes (B_1... B_i) pour échanger des informations chiffrées, et des moyens de traitement (10, 12, 13, 16, 20, 22, 24, 28, 30, 32, 34, 36, 38, 40, 46, 48, 52, 54) pour comparer lesdites informations chiffrées avec lesdites informations spécifiques et autoriser la collecte en fonction des résultats de la comparaison.



EP 0 413 636 A1

SYSTEME ET PROCEDE POUR CONTROLER LA COLLECTE DE BORNES A PREPAIEMENT

La présente invention a pour objet un système et un procédé pour sécuriser et contrôler la collecte de bornes à prépaiement notamment de bornes de stationnement payant pour véhicules.

Des bornes à prépaiement sont utilisées par exemple pour la délivrance d'objets divers tels que timbres, tickets... ou l'obtention de services (taxe de transport...), en échange de pièces de monnaie. Une application plus particulière concerne les bornes de stationnement payant pour véhicules. Il est bien connu que, sur les voies publiques, en particulier dans les grandes agglomérations, le stationnement payant en fonction du temps de stationnement du véhicule s'est beaucoup développé. En d'autres termes, pour pouvoir laisser en stationnement son véhicule, pendant un certain temps, l'automobiliste doit prépayer un montant donné pour être autorisé à stationner effectivement.

Ll'automobiliste qui veut stationner sur l'un des emplacements contrôlés par une borne de stationnement placée sur le trottoir, introduit dans la borne des pièces de monnaie pour un montant correspondant au temps de stationnement désiré.

Ces bornes de stationnement comportent un coffre qui peut être du type décrit dans le brevet français 2484674 déposé le 11 juin 1980 au nom du demandeur, pour le stockage temporaire des pièces de monnaie introduites dans les bornes avant leur transfert dans un dispositif de collecte. Une partie du coffre est constituée par la borne elle-même et présente un orifice de collecte normalement obturé par un obturateur, qui est lui-même bloqué par le pène d'une serrure d'accès à l'orifice de collecte, le pène étant manoeuvrable uniquement à l'aide d'une clé physique par le personnel de collecte. La clé physique introduite dans la serrure, efface le pène correspondant, libérant complètement l'obturateur. L'orifice de collecte étant ainsi dégagé, le dispositif de collecte, décrit lui aussi dans la demande précitée, préalablement disposé en vis-à-vis de l'orifice de collecte, récupère par effet de gravité les pièces de monnaie accumulées dans le coffre de la borne, par utilisation d'un flexible, à travers l'ouverture dégagée par l'obturateur.

Un des inconvénients est que le personnel de collecte, dûment autorisé à posséder la clé physique pour ouvrir le coffre, peut frauduleusement détourner une partie de la collecte, c'est-à-dire des pièces de monnaie stockées dans le coffre, au cours du transfert de ces pièces de monnaie du coffre dans le dispositif de collecte via le flexible. En effet, une fois le coffre complètement vidé, le personnel de collecte peut récupérer frauduleusement les pièces de monnaie encore contenues dans le flexible, ou se servir directement dans le dispositif de collecte. Le problème est qu'on ne peut pas détecter le vol de ces pièces de monnaie au cours de la collecte et qu'on ne peut pas en déterminer les auteurs. Cette collecte frauduleuse peut être qualifiée de "détournée".

Pour accroître la sécurité de collecte de bornes à prépaiement, un objet de l'invention est de fournir un système supplémentaire de protection, qui s'ajoute à l'utilisation de la clé physique, permettant de diminuer le risque d'une collecte détournée en dissuadant le personnel de collecte de voler des pièces de monnaie au cours de la collecte.

Pour atteindre ce but, selon l'invention, le système pour sécuriser et contrôler la collecte de bornes à prépaiement, est caractérisé en ce qu'il comprend un centre de collecte, des bornes (B_1 ...B_i) comprenant chacune un coffre pour le stockage temporaire des pièces de monnaie introduites dans ladite borne et des moyens de mémorisation pour mémoriser des informations spécifiques à chaque borne B_i, des moyens de dialogue entre ledit centre de collecte et lesdites bornes (B_1 ... B_i) pour échanger des informations chiffrées, et des moyens de traitement pour comparer lesdites informations chiffrées avec lesdites informations spécifiques et autoriser la collecte en fonction des résultats de la comparaison.

Selon un mode préféré de réalisation, le système comprend

- des moyens externes auxdites bornes (B_1...B_i) pour générer des messages de commande comportant notamment des informations d'identification du personnel de collecte et lesdites informations spécifiques ;
- des moyens pour chiffrer lesdits messages de commande ;
- des moyens pour transmettre lesdits messages de commande chiffrés vers lesdites bornes (B_1...B_i) ;
- des moyens situés dans chaque borne (B_1...B_i) pour déchiffrer ledit message de commande chiffré correspondant à ladite borne et pour valider ledit message de commande déchiffré ; et
- des moyens situés dans chaque borne (B_1.....B_i) pour délivrer un signal de commande à un moyen mécanique permettant l'ouverture dudit coffre .
- des moyens situés dans chaque borne (B_1...B_i) pour générer des messages de retour comportant des informations sur le montant des pièces de monnaie contenues dans ledit coffre de ladite borne (B_i) avant la collecte et lesdites informations d'identification du personnel de collecte reçues, et pour chiffrer lesdits messages de retour ;
- des moyens pour transmettre lesdits messages

de retour d'informations chiffrés vers ledit centre de collecte ;
- des moyens situés dans ledit centre de collecte pour déchiffrer lesdits messages de retour chiffrés et pour les valider ;
- des moyens situés dans ledit centre de collecte pour comparer ledit montant de pièces de monnaie contenu dans lesdits messages de retour déchiffrés avec celui des pièces de monnaie résultant de la collecte physique ; et
- des moyens situés dans ledit centre de collecte pour traiter les résultats de cette comparaison afin de détecter un éventuel vol de pièces de monnaie au cours de la collecte s'il n'y a pas correspondance de valeur entre lesdits deux montants à une valeur d'erreur près donnée, et pour identifier le personnel de collecte auteur du vol par connaissance des informations d'identification contenues dans lesdits messages de retour.

Le procédé pour sécuriser et contrôler la collecte de bornes à prépaiement est caractérisé en ce qu'il comprend les étapes suivantes :
- on fournit un centre de collecte ;
- on fournit des bornes (B_1...B_i) comprenant chacune un coffre pour le stockage temporaire des pièces de monnaie introduites dans ladite borne et des moyens de mémorisation pour mémoriser des informations spécifiques à chaque borne B_i ;
- On fournit des moyens de dialogue entre ledit centre de collecte et lesdites bornes (B_1...B_i) pour échanger des informations chiffrées ;
- On compare lesdites informations chiffrées avec lesdites informations spécifiques ; et
- on autorise la collecte en fonction des résultats de la comparaison.

Selon un mode préféré de mise en oeuvre de l'invention, les bornes sont des bornes pour la gestion du stationnement payant des véhicules.

D'autres caractéristiques et avantages de l'invention apparaîtront plus clairement à la lecture de la description qui suit de plusieurs modes de mise en oeuvre de l'invention donnés à titre d'exemples non limitatifs. La description se réfère au dessin annexé sur lequel :

La figure unique est une vue en bloc diagramme d'un mode de mise en oeuvre du système de contrôle de la collecte selon l'invention.

En se référant à la figure unique, on va décrire un mode de réalisation du système pour contrôler la collecte de bornes à prépaiement, notamment de bornes de stationnement payant pour véhicules. Le système comporte essentiellement un centre de collecte 10, comprenant entre autres un microordinateur 12, ayant pour rôle de sécuriser et contrôler la collecte de bornes de stationnement, un réseau de bornes de stationnement B_1... B_i comportant chacune une fente 14 pour l'introduction de pièces de monnaie. Les pièces introduites dans la fente 14 sont contrôlées par un sélecteur de pièces 16 qui détecte le montant effectif introduit dans la fente 14. Bien entendu, après être passées dans le sélecteur de pièces 16, les pièces de monnaie sont stockées temporairement dans un coffre 18, décrit précédemment, avant leur transfert dans un dispositif de collecte.

Le système comporte de plus un terminal portable 24, porté par le préposé chargé de la collecte des bornes B_1...B_i assurant la liaison et l'échange d'informations entre le centre de collecte 10 et le réseau de bornes B_1...B_i.

On envoie une clé logique (suite ordonnée d'un certain nombre de bits) caractéristique de chacune des bornes du réseau, du centre de collecte à la borne considérée par l'intermédiaire du terminal portable 24. Si la clé logique est cohérente avec un certain nombre de critères ou données mémorisés dans la borne, l'électronique de la borne va commander l'ouverture du coffre stockant les pièces de monnaie en actionnant un moyen mécanique d'ouverture. La clé logique n'est en fait valide que pendant la durée de la collecte car le coffre ne peut être ouvert que s'il y a identité d'un certain nombre de données entre celles contenues dans la borne et celles contenues dans la clé logique. La clé physique toutefois peut exister pour accroître la sécurité.

Pour fonctionner, le système doit obéir à deux impératifs. Il faut que la clé logique, si elle peut être modifiée au cours de son transfert entre le centre de collecte 10 et la borne considérée via le terminal 24, ne soit pas cohérente avec les critères mémorisés dans la borne et donc non validée par la borne, empêchant ainsi l'ouverture du coffre, et donc la collecte. Il faut d'autre part que le coffre de la borne authentifie la clé logique spécifique comme provenant effectivement du centre de collecte. Pour signer son intervention, le centre de collecte génère des clés logiques, utilisant une technique de chiffrement.

Le centre de collecte 10, par l'intermédiaire du microordinateur 12 sélectionne une équipe de collecte et un circuit de collecte pour un réseau de bornes B_1... B_i.

Les numéros de série de chaque borne du réseau sont mémorisés dans la mémoire 13 du microordinateur 12. Un programme du microordinateur 12 génère les messages de commande en clair pour chaque borne du réseau (message MC), c'est à dire les clés logiques en clair. Chaque message de commande comprend un message d'informations fonction de l'équipe de collecte, de la date, du numéro de série de la borne considérée et d'un indice R spécifique à chaque borne B_i dont la fonction sera décrite ultérieurement suivi de l'ordre pour relever le montant de pièces de monnaie contenues dans le coffre de la borne considérée,

ledit montant étant mémorisée dans cette borne et de l'ordre d'ouverture de coffre. L'indice R et le numéro de série spécifiques à chaque borne B_i constituent ce qu'on appelle les informations spécifiques à la borne B_i.

Ce message d'informations est par exemple de la forme : /Equipe collecte 23/11mars 1989/Borne n° 46 281/R.

Ces messages de commande sont ensuite chiffrés ou cryptés dans le microordinateur 12 en utilisant la fonction R.S.A. de cryptage ou chiffrement à clé publique. Cette fonction comprend une clé secrète d_1, et un couple (e,n_1) formant clé publique, supposée connue. Dans le mode de réalisation décrit, la clé d_1 et le couple (e,n_1) sont utilisés pour chiffrer les messages de commande de toutes les bornes d'un même réseau, mais on peut tout aussi bien envisager une clé secrète d et un couple (e,n) spécifiques à chaque borne du réseau. Le message de commande (MC), ainsi chiffré par l'utilisation de la clé secrète d_1 et du couple (e, n_1), est transformé en un message de commande chiffré ou signé (MC chiffré) correspondant à la clé logique définie précédemment. Dans le centre 10, on peut schématiser le chiffrement par la formule

MC^{d1} modulo (n_1) = MC chiffré.

Une carte à mémoire électronique 20, dans le centre 10, mémorise le couple clé secrète - clé publique (d_1, n_1), e mémorisé dans la mémoire 13 étant égal à trois dans le mode réalisation décrit, protégée en lecture par une clé propre et un code confidentiel . La carte 20 est ensuite introduite dans le lecteur de carte 22 qui est lui-même connecté au microordinateur 12.

Le microordinateur 12 pour chiffrer un message de commande d'une borne B_i du réseau utilise la clé secrète d_1 mémorisée dans la carte 20 via le lecteur 22. Les messages de commande chiffrés ainsi obtenus, correspondant à chacune des bornes du réseau, sont stockés dans la mémoire 13. L'utilisation de la carte à mémoire électronique 20 permet de gérer les opérations de chiffrement sans que l'utilisateur préposé au centre de collecte connaisse la valeur de la clé secrète d_1. La carte à mémoire 20, support de la clé secrète d_1, peut être confiée à un seul employé de confiance responsable du centre de collecte 10, limitant ainsi les risques de connaissance frauduleuse de la clé d_1.

En effet, la connaissance de la clé secrète d_1 permet de chiffrer n'importe quel message de commande, et la borne B_i via le terminal 24, reconnaissant la signature du centre 10, envoie un signal de commande pour l'ouverture du coffre si le message de commande comprend un ordre d'ouverture de coffre, ce qui est à l'opposé du but recherché, d'où l'intérêt d'un accès difficile à la clé secrète d_1, par exemple mémorisée dans une carte à mémoire électronique 20.

Le terminal portable 24 porté par le préposé chargé de la collecte comprend un circuit électronique 42 avec une mémoire de stockage 26. La recopie dans la mémoire de stockage 26 du terminal portable 24 des messages de commande chiffrés correspondant à chaque borne B_i ou clés logiques stockés dans la mémoire 13 du microordinateur 12, peut se faire par liaison filaire, par rayonnement infrarouge ou tout autre type de liaison capable de transmettre des informations. Dans le cadre du mode de réalisation par transmission infrarouge, le terminal 24 est muni d'un émetteur-récepteur infrarouge 28 pour dialoguer avec le centre 10 qui est également muni d'un émetteur-récepteur infrarouge 30. Un tel système est décrit dans la demande de brevet européen n° 84/401799.

La borne B_i comprend un microprocesseur 32 qui gère l'ensemble de ses fonctions comprenant une mémoire 34. Le microprocesseur 32 et la mémoire 34 forme la carte principale 46 de la borne B_i.

Le coffre 18 de la borne B_i comprend un microprocesseur 40 avec une mémoire 38 mémorisant entre autres informations le numéro de série de ladite borne B_i, le microprocesseur 40 étant relié au microprocesseur 32 de la borne B_i. La carte principale 46 joue le rôle d'intermédiaire entre le terminal 24 et le microprocesseur 40 du coffre 18.

Le signal délivré par le sélecteur de pièces 16, représentatif du montant de pièces de monnaie introduites par la fente 14 de la borne B_i est envoyé au microprocesseur 32 de la carte principale 46 qui calcule le montant correspondant de pièces de monnaie. Ce montant est ensuite additionné au montant global de pièces de monnaie déjà introduites dans le coffre 18 via la fente 14, ledit montant global étant mémorisé dans la mémoire 34. Ce montant global est ensuite envoyé périodiquement, par exemple quotidiennement, dans la mémoire 38 du microprocesseur 40 du coffre 18 en venant écraser la valeur du montant global précédemment envoyé du microprocesseur 32 dans la mémoire 38 du coffre. D'autres informations sont mémorisées dans la mémoire 34 comme par exemple l'état de la pile d'alimentation de la borne B_i délivré par le dispositif 44 et la date.

Le préposé à la collecte présente le terminal portable 24 à la borne B_i. Par transmission infrarouge et par activation de l'émetteur-récepteur infrarouge 36 de la borne B_i, ou par tout autre moyen de transmission, le terminal 24 envoie un ordre de lecture du numéro de série à la carte principale 46 de la borne B_i. En réponse, le terminal 24 par l'intermédiaire de son circuit électronique 42 reçoit le numéro de série de la borne B_i considérée,

envoyé par le microprocesseur 40 via la carte principale 46. Le circuit électronique 42 du terminal portable 24 compare le numéro de série reçu de la borne B_i considérée avec une liste préenregistrée dans la mémoire 26 du circuit électronique 42 de numéros de série des bornes auxquelles est adressé un message de commande chiffré. Cette liste préenregistrée de numéros de série élaborée par le centre de collecte 10, est chargée dans la mémoire 26 du circuit électronique 42 du terminal 24 lors de la transmission des messages de commande chiffrés du centre de collecte vers le terminal 24. S'il y a correspondance de valeur entre le numéro de série reçu et un des numéros de série contenus dans la liste préenregistrée, le terminal 24 transmet par les moyens 28 et 36 le message de commande chiffré correspondant ou clé logique vers la carte principale 46 de la borne B_i. Cette clé logique est ensuite transmise de la carte principale 46 vers la mémoire 38 du microprocesseur 40 du coffre 18 pour y être déchiffrée. Cette opération de déchiffrement de la clé logique ne peut s'effectuer qu'à l'intérieur du coffre 18 par le microprocesseur 40, qui ne doit pas être accessible au personnel de collecte, et non dans la carte principale 46 auquelle le personnel de collecte a accès en pratique. Par utilisation de la olé publique (e, n_1) mémorisée dans la mémoire 38, la clé logique ou message de commande chiffré correspondant à la borne B_i, est déchiffré par le microprocesseur 40 du coffre qui génère le message de commande en clair (message MC). Dans le coffre, on peut schématiser le déchiffrement de la clé logique par la formule $(\text{MC chiffré})^e \text{ modulo } (n_1) = \text{MC}$.

La validation du message MC en clair est effectuée par le microprocesseur 40 du coffre en comparant la valeur de l'indice R mémorisée dans la mémoire 38 du coffre 18 avec celle de l'indice R contenue dans le message d'informations du MC en clair et en comparant le numéro de série de la borne B_i mémorisé dans la mémoire 38 du coffre avec celui contenu dans le message d'informations. S'il y a correspondance de valeur, le microprocesseur 40 envoie un message de retour d'informations chiffré au terminal 24 via la carte principale 46 qui est la réponse à l'ordre pour relever le montant de pièces de monnaie contenu dans le message de commande. Par ailleurs, si le message de commande MC contient l'ordre d'ouverture de coffre, le microprocesseur 40 envoie un signal à une électronique de commande, commandant un moyen mécanique d'ouverture du coffre 18, en l'occurence une tige métallique qui se trouve sur la course de dégagement du pène de la serrure précédemment décrite manoeuvrable par la clé physique. La tige, actionnée par l'électronique 48, perpendiculaire au pène de la serrure, effectue un mouvement vertical de telle sorte qu'elle se trouve entièrement au-dessus du plan contenant le pène. Le pène, dont la course de dégagement est ainsi libérée, peut être actionnée par la clé physique.

Cela provoque aussi l'envoi d'un message sur l'écran 50 du terminal 24 à l'adresse du préposé à la collecte dont l'intitulé est "introduisez la clé physique", par l'intermédiaire des microprocesseurs 40 et 32 de la borne B_i.

A compter de la validation du MC par le microprocesseur 40, une temporisation d'une durée déterminée démarre, pendant laquelle le préposé à la collecte, prévenu par l'apparition du message sur l'écran 50 du terminal 24, doit introduire la clé physique permettant d'actionner le pène libérant l'obturateur. Pendant la durée de cette temporisation, la tige métallique se trouve en position haute par rapport au pène. A la fin de la temporisation, la tige revient à sa position initiale, bloquant le pène de la serrure, de sorte que si on veut collecter de nouveau la borne B_i, il faut attendre l'envoi d'une nouvelle clé logique avec l'indice R correct, par le relais du terminal 24, car la fin de la temporisation provoque aussi la modification de l'indice R mémorisé dans la mémoire 38, par l'utilisation d'un algorithme mémorisé dans la mémoire 38 du microprocesseur 40 du coffre 18. Cette modification peut être une incrémentation d'une unité de l'indice R. Cette modification de l'indice R permet de rendre inutilisable les clés logiques des collectes précédentes pour la borne B_i, car dans ce cas-là la non correspondance des valeurs des indices R contenus dans les clés logiques déchiffrées et la mémoire 38 du microprocesseur 40 ne permet pas la validation du message de commande. De ce fait même si le message de commande contient l'ordre d'ouverture de coffre, le microprocesseur 40 n'envoie pas un signal à l'électronique de commande 48, la tige métallique reste dans sa position, ne permettant pas le dégagement du pène et donc le coulissement de l'obturateur, même si la personne mal intentionnée a en sa possession la clé physique. La modification de l'indice R provoque aussi la mise à zéro du montant global de pièces de monnaie contenues dans le coffre 18, mémorisé dans la mémoire 34.

Le MC chiffré ou la clé logique doit au-moins être intègre, c'est-à-dire qu'il ou elle n'apu être chiffré que par le centre de collecte 10, cette signature par utilisation de la clé d_1 étant authentifiée par le microprocesseur 40 du coffre 18 de la borne B_i. Un éventuel fraudeur pourra connaître la contenu du message MC en clair car le couple (e,n) forme clé publique et que MC chiffré peut être frauduleusement lu dans le terminal 24, mais il ne pourra pas fabriquer des MC chiffrés sans la connaissance de la clé d_1.

Dans un deuxième temps, on va aborder le problème de la détection du vol de pièces de

monnaie au cours de la collecte et de la prévention de la collecte "détournée". On a déjà signalé ci-avant que la présence de l'ordre pour relever le montant de pièces de monnaie dans le message de commande provoque l'envoi d'un message de retour d'informations chiffré de la borne B_i dans le terminal 24 dont la création est décrite ci-après. Le microprocesseur 40 du coffre 18 génère un message de retour d'informations en clair (message RICL) composé d'informations mémorisées dans sa mémoire 38 ou dans la mémoire 34 de la carte principale 46 telles que des informations sur l'identification du personnel de collecte, la date, le numéro de série de la borne B_i collectée, le montant des pièces de monnaie contenues dans le coffre 18, ou encore des données liées à la maintenance ou tout autre information. Ce message RICL peut se présenter sous la forme :
Equipe collecte 23/11 mars 1989/borne n° 46 281/Somme 5250 FF/

Pour générer le message RICl, le microprocesseur 40 du coffre 18, une fois déchiffré le MC chiffré, récupère l'information sur l'identification du personnel de collecte (ex : Equipe Collecte 23) contenue dans le MC en clair, pour l'intégrer dans le message RICL.

Le message RICL est ensuite chiffré ou crypté au niveau du microprocesseur 40 en utilisant la fonction D.E.S. (Data Encription Standard) de cryptage ou chiffrement à clé symétrique k qui doit rester secrète. Le message RICL, chiffré par l'utilisation de la clé secrète k mémorisée au niveau de la mémoire 38, est transformé en un message de retour d'informations chiffré (message RICH). On peut schématiser le chiffrement du RICL au niveau du microprocesseur 40 par la formulation :
DES (k, RICL) = RICH

Le DES consiste à effectuer des permutations et certaines opérations non linéaires sur les bits du message à chiffrer. Ces manipulations de bits sont paramétrés par k.

Le RICH ainsi obtenu, est transféré dans la mémoire 26 du terminal 24 via la carte principale 46. Dès que le préposé ou l'équipe de collecte a collecté l'ensemble des bornes B_1... B_i du circuit de collecte préalablement défini, il ou elle retourne au centre de collecte 10 et effectue le transfert des messages de retour d'informations chiffrés des bornes B_1.... B_i effectivement collectées du circuit de collecte, de la mémoire 26 du microprocesseur 42 du terminal 24 dans la mémoire 13 du microordinateur 12 du centre de collecte 10 par l'intermédiaire des moyens 30 et 28, ou de tout autre moyen de transmission terminal portable - centre de collecte.

Lors de l'initialisation du système, le centre de collecte (10) génère des ordres d'initialisation en clair spécifiques à chacune des bornes B_i, qui sont envoyés dans le microprocesseur 40 de chaque coffre 18 des bornes B_i pour y être traités, via le terminal portable 24 et la carte principale 46. Chacun de ces ordres contient le numéro de série de la borne considérée, la clé k de la fonction DES, la clé publique (e, n_1) de la fonction RSA et l'indice R qui est égal à un. Dès que le microprocesseur 40 du coffre 18 reçoit cet ordre d'initialisation spécifique à la borne B_i, il stocke dans sa mémoire 38 les informations contenues dans l'ordre d'initialisation telles que la clé k, la clé (e,n_1), la valeur de l'indice R et le numéro de série de la borne considérée.

Par utilisation de la clé secrète k mémorisée dans de la carte à mémoire 20 introduite dans le lecteur de carte 22, le microordinateur 12 déchiffre les messages RICH de chacune des bornes B_i aboutissant à la restitution des messages de retour d'informations en clair RICL de chacune des bornes B_i. Dans le microordinateur 12, le déchiffrement des messages RICH se présente sous la forme :
DES^{-1} (k, RICH) = RICL.

Seule la connaissance de la clé secrète k permet de chiffrer ou déchiffrer les messages RICL ou RICH. De ce fait, la fonction DES assurent les propriétés de confidentialité et d'intégrité des informations contenues dans les messages de retour chiffrés.

Un circuit de traitement 52 relié au microordinateur 12 calcule le montant global de pièces de monnaie théoriquement contenues dans l'ensemble des coffres des bornes B_1...B_i effectivement collectées du circuit de collecte en additionnant les montants de pièces de monnaie théoriquement contenues dans chaque coffre des bornes B_i, indiqués dans les messages RICL de chacune des bornes B_i. Le circuit 52 traite aussi les autres informations contenues dans les messages RICL.

Pour détecter le vol des pièces de monnaie au cours de la collecte des bornes B_1... B_i du circuit de collecte, il suffit de comparer le montant des pièces de monnaie effectivement contenues dans le chariot de collecte issues de la collecte des bornes B_1... B_i avec le montant global de pièces de monnaie théoriquement contenues dans chaque borne B_i. Cette comparaison est effectuée par le comparateur 54 et les résultats de cette comparaison sont traités par le circuit de traitement 52. Si ces deux montants sont égaux à un pourcentage d'erreur près donné, il n'y a pas eu de vol au cours de cette collecte pour le circuit de collecte donné. Par contre, si la différence entre les deux montants est supérieure au pourcentage d'erreur donné, cela indique qu'un vol de pièces de monnaie a été effectué au cours de cette collecte et ce vol est ainsi détecté. Les auteurs de ce vol peuvent être facilement identifiés par les indications contenues dans les messages de retour d'informations sur

l'équipe de collecte.

Cette détection de vol de pièces de monnaie au cours de la collecte peut ainsi prévenir la collecte qualifiée de "détournée".

La valeur de l'indice R précédemment mentionné, est mémorisée dans la mémoire 13 du microordinateur 12. Dès que la microordinateur 12 reçoit les messages de retour d'informations, la valeur de l'indice R spécifique à chaque borne B_i est écrasée par la nouvelle valeur de l'indice R spécifique à chaque borne B_i contenue dans les messages de retour d'informations, et c'est cette nouvelle valeur R spécifique qui sera intégrée dans les prochains messages de commande des bornes B_1... B_i de ce circuit de collecte. La validation du message de commande dans la borne B_i pourra s'effectuer, car la correspondance de la valeur de l'indice R contenu dans la borne et celle du R contenu dans le message de commande correspondant sera effective.

Il est possible que des fraudeurs arrivent à casser le cryptosystème, c'est à dire à connaître la clé secrète d_1 de la fonction RSA et la clé secrète k de la fonction DES, soit par des attaques cryptanalytiques, soit en lisant directement la clé secrète d_1 dans la carte à mémoire 20 du centre de collecte 10 ou en lisant la clé secrète k dans le coffre 18 ou le centre de collecte 10. La lecture des clés secrètes est catastrophique car le fraudeur peut alors collecter les bornes B_1... B_i du circuit de collecte concerné ou introduire de fausses informations, notamment sur le montant des pièces de monnaie contenues dans le coffre 18, dans le message de retour envoyé par la borne B_i vers le centre de collecte 10 via le terminal 24.

Pour remédier à ce problème, il a été prévu lors de l'initialisation du système de mémoriser des clés de rechange dans le centre de collecte et dans le coffre 18 de la borne B_i. Concernant la fonction RSA, la carte à mémoire 20 mémorise le couple de clés (d_2, n_1) qui est effectivement utilisé pour chiffrer le message d'ouverture du coffre, mais aussi d'autres couples de clé (d_1, n_2), (d_3, n_3).. qui peuvent jouer le rôle de clés de rechange au cas où la clé secrète d_1 est connue d'un fraudeur. Chaque couple de clés (d_2, n_2), (d_3, n_3) peut être mémorisé dans une carte à mémoire spécifique.De même dans le coffre 18, la mémoire 38 mémorise la clé publique n_1 qui est effectivement utilisée, mais aussi d'autres clés publiques de rechange n_2, n_3..., e restant toujours égal à 3. Ces clés publiques de rechange n_2, n_3 sont mémorisées dans la mémoire 38 du coffre 18 par l'intermédiaire du terminal portable 24 lors de la phase d'initialisation par l'envoi d'un ordre d'initialisation en clair, précédemment défini, par le centre de collecte (10) vers la borne B_i. A partir du moment où on a la certitude que la clé secrète d_1 est connue d'un fraudeur, le centre de collecte 10 envoie via le terminal 24 un ordre chiffré par (d_1, n_1) vers le microprocesseur 40 du coffre 18 lui commandant d'utiliser dorénavant la clé publique suivante mémorisée dans la mémoire 38, en l'occurence n_2, pour déchiffrer les messages de commande. De même au niveau du centre de collecte 10, le microordinateur 12 utilisera dorénavant pour chiffrer les messages de commande le couple de clés suivant mémorisé dans la carte à mémoire 20, ou mémorisé dans une autre carte à mémoire, en l'occurence (d_2, n_2).

Concernant la fonction D.E.S., la clé secrète k est mémorisée dans la carte à mémoire 20 et dans la mémoire 38 du coffre 18. En cas de connaissance frauduleuse, la clé k doit être changée. Le microordinateur 12 commande l'effacement de la clé k dans la carte à mémoire 20 et l'inscription dans cette même carte de la nouvelle clé k. Il envoie un ordre chiffré par la fonction RSA de changement de la clé k, contenant le chiffrement DES de la la nouvelle clé k à l'aide de l'ancienne clé k, au microprocesseur 40 du coffre 18 via le terminal 24. Le coffre 18, recevant cet ordre via le terminal 24, le déchiffre et la nouvelle clé k est inscrite dans la mémoire 38 du microprocesseur 40 à la place de l'ancienne clé k.

Lors de l'initialisation du système, la valeur de l'indice R pour chacune des bornes B_i mémorisé dans la mémoire 13 du microordinateur 12 du centre de collecte 10 est mise à un.

Revendications

1) Système pour sécuriser et contrôler la collecte de bornes à prépaiement (B_1...B_i) caractérisé en ce qu'il comprend un centre de collecte (10), des bornes (B_1...B_i) comprenant chacune un coffre (18) pour le stockage temporaire des pièces de monnaie introduites dans ladite borne et des moyens de mémorisation (34, 38) pour mémoriser des informations spécifiques à chaque borne B_i, des moyens de dialogue (24, 28, 30, 36) entre ledit centre de collecte (10) et lesdites bornes (B_1... B_i) pour échanger des informations chiffrées, et des moyens de traitement (10, 12, 13, 16, 20, 22, 24, 28, 30, 32, 34, 36, 38, 40, 46, 48, 52, 54) pour comparer lesdites informations chiffrées avec lesdites informations spécifiques et autoriser la collecte en fonction des résultats de la comparaison.

2) Système selon la revendication 1 caractérisé en ce que lesdits moyens de traitement (10, 12, 13, 20, 22, 24, 28, 30, 32, 34, 36, 38, 40, 48) comprennent :

- des moyens (10, 12, 13, 20, 22) externes auxdites bornes (B_1...B_i) pour générer des messages de commande comportant notamment des informa-

tions d'identification du personnel de collecte et lesdites informations spécifiques ;
- des moyens (12, 13) pour chiffrer lesdits messages de commande ;
- des moyens (24, 28, 30, 32, 34, 36, 46) pour transmettre lesdits messages de commande chiffrés vers lesdites bornes (B_1...B_i) ;
- des moyens (38, 40) situés dans chaque borne (B_1...B_i) pour déchiffrer ledit message de commande chiffré correspondant à ladite borne et pour valider ledit message de commande déchiffré ; et
- des moyens (48) situés dans chaque borne (B_1.....B_i) pour délivrer un signal de commande à un moyen mécanique permettant l'ouverture dudit coffre (18) .

3) Système selon la revendication 2 caractérisé en ce que lesdits moyens de traitement (10, 12, 13, 16, 24, 28, 30, 32, 34, 36, 38, 40, 46, 52, 54) comprennent de plus:
- des moyens (16, 38, 40, 44) situés dans chaque borne (B_1...B_i) pour générer des messages de retour comportant des informations sur le montant des pièces de monnaie contenues dans ledit coffre (18) de ladite borne (B_i) avant la collecte et lesdites informations d'identification du personnel de collecte reçues, et pour chiffrer lesdits messages de retour ;
- des moyens (24, 28, 30, 32, 34, 36, 46) pour transmettre lesdits messages de retour d'informations chiffrés vers ledit centre de collecte (10) ;
- des moyens (12, 13) situés dans ledit centre de collecte (10) pour déchiffrer lesdits messages de retour chiffrés et pour les valider ;
- des moyens (54) situés dans ledit centre de collecte (10) pour comparer ledit montant de pièces de monnaie contenu dans lesdits messages de retour déchiffrés avec celui des pièces de monnaie résultant de la collecte physique ; et
- des moyens (52) situés dans ledit centre de collecte (10) pour traiter les résultats de cette comparaison afin de détecter un éventuel vol de pièces de monnaie au cours de la collecte s'il n'y a pas correspondance de valeur entre lesdits deux montants à une valeur d'erreur près donnée, et pour identifier le personnel de collecte auteur du vol par connaissance des informations d'identification contenues dans lesdits messages de retour.

4) Système selon l'une quelconque des revendications 2 et 3 caractérisé en ce que lesdits moyens (38, 40) de validation dudit message de commande déchiffré comprennent des moyens (38, 40) pour comparer la valeur d'un numéro de borne B_i correspondant à une desdites informations spécifiques, contenue dans ledit message déchiffré avec la valeur du numéro de borne B_i mémorisé dans lesdits moyens de mémorisation (34, 38), et des moyens (40) pour traiter les résultats de cette comparaison afin de valider ledit message de commande déchiffré en fonction des résultats de ladite comparaison.

5) Système selon l'une quelconque des revendications 2,3 et 4 caractérisé en ce que lesdits moyens (38, 40) de validation dudit message de commande déchiffrée comprennent des moyens (38, 40) pour comparer la valeur d'un indice R correspondant à une desdites informations spécifiques,contenue dans ledit message de commande déchiffrée avec la valeur de l'indice R mémorisé dans lesdits moyens de mémorisation (34, 38), des moyens (40) pour traiter les résultats de cette comparaison afin de valider ledit message de commande déchiffré en fonction des résultats de ladite comparaison, et des moyens (38, 40) pour modifier ledit indice R mémorisé dans lesdits moyens de mémorisation (34, 38) à la fin de chaque collecte réalisée de sorte que les messages de commande des précédentes collectes ne sont plus valables et ne peuvent pas être validées.

6) Système selon la revendications 3 caractérisé en ce que lesdits moyens de mémorisation (34, 38) comprennent une mémoire (38) et un microprocesseur (40) situés dans le coffre de chacune des bornes B_i et non accessibles au personnel de collecte, mémorisant notamment le montant des pièces de monnaie contenues dans ledit coffre (18).

7) Système selon l'une quelconque des revendications 1 à 5 caractérisé en ce que lesdits moyens de mémorisation (34,38) comprennent une mémoire (38) et un microprocesseur (40) situés dans le coffre de chacune des bornes B_i et non accessibles au personnel de collecte, mémorisant notamment lesdites informations spécifiques.

8) Système selon l'une quelconque des revendications 1 à 7 caractérisé en ce que lesdites bornes à prépaiement (B_1...B_i) sont des bornes de stationnement payant.

9) Système selon l'une quelconque des revendications 1 à 8 caractérisé en ce que lesdits moyens de dialogue comprennent un terminal portable (24) comprenant un écran (50), un circuit électronique (42), une mémoire (26) pour mémoriser lesdites informations chiffrées et des moyens de transmission (28) avec ledit centre de collecte (10) et ladite borne B_i.

10) Système selon l'une quelconque des revendications 2 à 9 caractérisé en ce que lesdits messages de commande sont chiffrés par un algorithme à clé secrète et à clé publique, ladite clé secrète étant mémorisée dans ledit centre de collecte (10) et ladite clé publique mémorisée à la fois dans ledit centre de collecte (10) et dans chaque borne B_i.

11) Système selon l'une quelconque des revendications 3 à 9 caractérisé en ce que lesdits messages de retour sont chiffrés par un algorithme à clé

secrète, ladite clé secrète étant mémorisée dans ledit centre de collecte (10) et dans chaque borne B_i.

12) Procédé pour sécuriser et contrôler la collecte de bornes à prépaiement (B_1...B_i) caractérisé en ce qu'il comprend les étapes suivantes :

- on fournit un centre de collecte (10) ;
- on fournit des bornes (B_1...B_i) comprenant chacune un coffre (18) pour le stockage temporaire des pièces de monnaie introduites dans ladite borne et des moyens de mémorisation (34, 38) pour mémoriser des informations spécifiques à chaque borne B_i ;
- On fournit des moyens de dialogue (24, 28, 30, 36) entre ledit centre de collecte (10) et lesdites bornes (B_1...B_i) pour échanger des informations chiffrées ;
- On compare lesdites informations chiffrées avec lesdites informations spécifiques ; et
- on autorise la collecte en fonction des résultats de la comparaison.

13) Procédé selon la revendication 12 caractérisé en ce que les étapes de comparaison et d'autorisation comprennent les étapes suivantes :

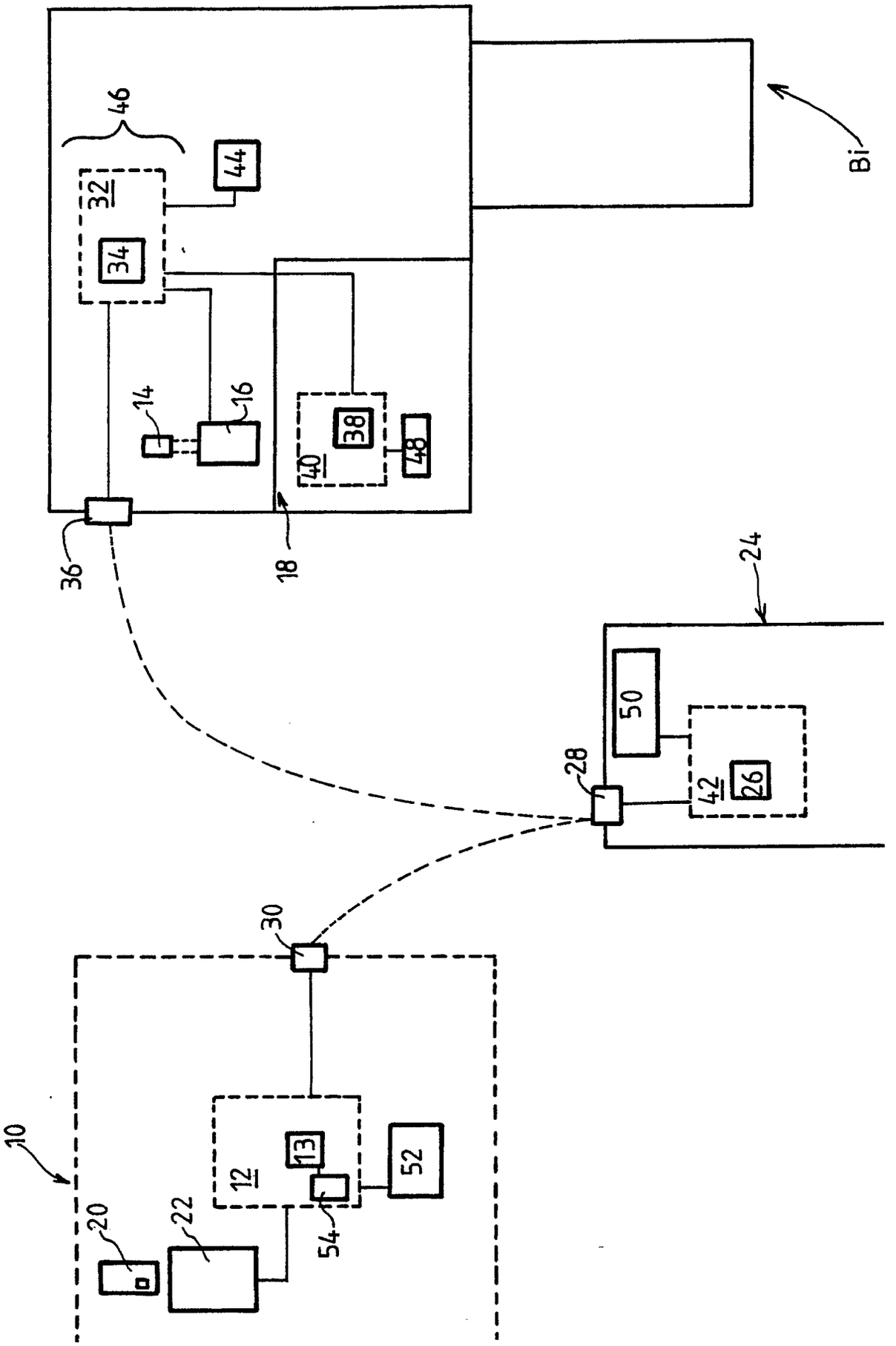
- On génère à l'externe desdites bornes (B_1...B_i) des messages de commande comportant notamment des informations d'identification du personnel de collecte et lesdites informations spécifiques;
- On chiffre lesdits messages de commande ;
- On transmet lesdits messages de commande chiffrés vers lesdites bornes (B_1... B_i) ;
- On déchiffre dans chaque borne (B_1...B_i) ledit message de commande chiffré correspondant à ladite borne et on valide ledit message de commande chiffré ; et
- On envoie par des moyens (48) situés dans chaque borne (B_1...B_i) un signal de commande à un moyen mécanique permettant l'ouverture dudit coffre (18).

14) Procédé selon la revendication 13 caractérisé en ce que les étapes de comparaison et d'autorisation comprennent de plus les étapes suivantes :

- On génère dans chaque borne (B_1... B_i) des messages de retour comportant des informations sur le montant des pièces de monnaie contenues dans ledit coffre (18) de ladite borne (B_i) avant la collecte et lesdites informations d'identification du personnel de collecte reçues, et on chiffre lesdits messages de retour ;
-On transmet lesdits messages de retour d'informations chiffrés vers ledit centre de collecte (10) ;
-On déchiffre dans ledit centre de collecte (10) lesdits messages de retour chiffrés et on les valide ;
-On compare dans ledit centre de collecte (10) ledit montant de pièces de monnaie contenu dans lesdits messages de retour déchiffrés avec celui des pièces de monnaie résultant de la collecte physique ; et
-On traite dans ledit centre de collecte (10) les résultats de cette comparaison afin de détecter un éventuel vol de pièces de monnaie au cours de la collecte s'il n'y a pas correspondance de valeur entre lesdits deux montants à une valeur d'erreur près donnée, et pour identifier le personnel de collecte auteur du vol par connaissance des informations d'identification contenues dans lesdits messages de retour.

15) Procédé selon l'une quelconque des revendications 12 à 14 caractérisé en ce que lesdites bornes à prépaiement (B_1...B_i) sont des bornes de stationnement payant.

1 / 1


46
44
32
34
Bi
14
16
38
40
48
36
18
24
50
28
42
26
30
10
12
13
52
20
22
54

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande

EP 90 40 2298

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int. Cl.5)
Y	US-A-4 471 905 (SLOMA) * abrégé * - - -	1,12	G 07 F 9/06 G 07 F 17/24 G 07 B 15/00
Y,A	US-A-4 730 117 (ZACK) * le document en entier * - - - - -	1,12, 2-11, 13-15	

DOMAINES TECHNIQUES RECHERCHES (Int. Cl.5)

G 07 F

Le présent rapport de recherche a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
La Haye	13 novembre 90	TACCOEN J-F.P.L.

CATEGORIE DES DOCUMENTS CITES

- X : particulièrement pertinent à lui seul
- Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
- A : arrière-plan technologique
- O : divulgation non-écrite
- P : document intercalaire
- T : théorie ou principe à la base de l'invention
- E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
- D : cité dans la demande
- L : cité pour d'autres raisons

& : membre de la même famille, document correspondant