ROYAUME DE BELGIQUE

MINISTERE DES AFFAIRES ECONOMIQUES

BRE

BE 1008207A

NUMERO DE PUBLICATION : 1008207A6

NUMERO DE DEPOT : 09400950

Classif. Internat. : G07F

Date de délivrance le : 13 Février 1996

Le Ministre des Affaires Economiques,

Vu la loi du 28 Mars 1984 sur les brevets d'invention, notamment l'article 22;

Vu l' arrêté royal du 2 Décembre 1986 relatif à la demande, à la délivrance et au maintien en vigueur des brevets d'invention, notamment l'article 28;

Vu le procès verbal dressé le 20 Octobre 1994 à 14H40 à l 'Office de la Propriété Industrielle

ARRETE:

ARTICLE 1.- Il est délivré à : KABASELE TENDAY NDONDA
rue de l'Hocaille 15/102, B-1348 LOUVAIN-LA-NEUVE(BELGIQUE)

un brevet d' invention d' une durée de 6 ans, sous réserve du paiement des taxes annuelles, pour : TERMINAL INTELLIGENT POUR TRAITEMENT DES CARTES DIFFEREMMENT CODEES CONTENANT DES VALEURS A DEBITER ET/OU CREDITER LOCALEMENT.

ARTICLE 2.- Ce brevet est délivré sans examen préalable de la brevetabilité de l'invention, sans garantie du mérite de l'invention ou de l'exactitude de la description de celle-ci et aux risques et périls du(des) demandeurs(s).

Bruxelles, le 13 Février 1996
PAR DELEGATION SPECIALE :

WUYTS L
Directeur

Terminal Intelligent pour traitement des cartes différemment codées contenant des valeurs à débiter et/ou créditer localement .

L'invention concerne un terminal intelligent pour traitement des cartes différemment codées et à valeur(s) à débiter et/ou créditer localement, comprenant au moins une unité de lecture/écriture des cartes et un circuit de codage dans son unité centrale de traitement, capable d'authentifier ses cartes, de tester la validité du code de chacune d'elles, et enfin d'exécuter un traitement local, débiter et/ou créditer leurs valeurs, en cas de succès du test de validation. L'invention concerne également les cartes à codes et valeurs modifiables, appropriées pour ce genre de terminal.

Les modèles actuels des terminaux de traitement des cartes sont: les cabines téléphoniques, les terminaux des banques électroniques du genre Bancontact ou Mistercash, et les terminaux d'accès aux lieux ou à des biens protégés comme les bibliothèques, les laboratoires, les photocopieuses, etc. Les cabines téléphoniques authentifient localement leurs cartes, et les débitent pendant qu'elles servent à la communication. Leurs cartes n'ont pas des codes. Les terminaux des banques électroniques authentifient localement leurs cartes, mais sont tous reliés à un ordinateur central distant contenant un fichier avec les valeurs à débiter et/ou créditer ainsi que les codes de validité des cartes. Ils sont conçus au dessus d'un réseau de télécommunication qui leur assure la transmission des données et des commandes. Quand aux terminaux d'accès à des lieux ou à des biens, ils authentifient leurs cartes, selon les cas, débitent et/ou créditent un compteur distant, ou encore déclenchent un dispositif de sécurité...

On ne trouve pas des terminaux intelligents autonomes, c'est-à-dire des terminaux capable d'exécuter, sans recours à un ordinateur distant, tous les traitements essentiels de débits, crédits et tests de validité du code. Par ailleurs, les exigences de l'existence d'un réseau de télécommunication pour monter ces différents systèmes font qu'ils ne peuvent pas être opérationnels dans un endroit sous équipé,

ou bien ils exigeraient un énorme investissement préalable pour couvrir une large zone.

Le but de notre invention est de remédier à ces inconvénients. L'invention, telle qu'elle est caractérisée dans les revendications, résout le problème consistant à fabriquer les terminaux intelligents, capable de débiter et/ou créditer des cartes codées sans recours à un serveur central, lequel serveur est accédé via un réseau de télécommunication d'une part. Et des cartes codées à débiter et/ou créditer par ces terminaux d'autres part.

Les avantages obtenus grâce à cette invention consistent essentiellement en ceci qu'un réseau de télécommunication n'est pas indispensable alors que la contrainte de sécurité est respectée. Les opérations consistant à débiter et/ou créditer la carte sont localement exécutées par le terminal. Le système est dispensé des matériels et câbles divers pour être piloté.

L'invention est détaillée comme suit selon un mode d'exécution:

1. Le terminal est composée d'au moins une unité de lecture/écriture des cartes, d'une unité centrale contenant un circuit de codage représentant une fonction partielle "f" d'une fonction totale non inversible, dite fonction de codage, qui transforme un "mot de passe" en suite de symboles formant un code secret, d'un dispositif d'affichage et d'une unité d'impression. Pour éditer une nouvelle carte, son mot de passe est introduit, transformé via la fonction de codage. Le résultat de cette transformation est combiné avec le code exécutable de l'extension de la fonction "f" pour former un code. Ce code est inscrit de façon non détectable sur la carte ainsi qu'une marque d'authentification de la carte.

Le code sur la carte sera seulement lu par le terminal qui le place dans un registre du circuit de codage. Après authentification de la carte, un mot de passe sera saisi via le clavier, transformé en code par le circuit de codage, et comparé avec le code de la carte. En cas de succès, le terminal sera alors prêt à modifier les valeurs de

la carte en débit ou crédit grâce à son (ses) unité(s) de lecture/écriture. Sinon, un nombre limité de chances peuvent être accordées avant de declasser la carte pour contrôle.

Intégrer dans le terminal la possibilité de débiter et/ou créditer la carte est réalisée selon les mêmes principes que les cabines téléphoniques. Le codage des cartes est réalisé par écriture du code sur ces cartes.

2. La carte contient à son édition un code, rendu non détectable grâce à la combinaison d'une partie du code exécutable de la fonction de codage avec le résultat de la transformation du mot de passe par la fonction de codage. Elle contient aussi des valeurs qui sont modifiables, débitées et/ou créditées lors des utilisations dans les terminaux décrits ci-dessus. Un mode d'exécution de cette invention est soit une carte magnétique à deux bandes initialement vierges et une puce de code, soit une carte électronique à trois puces dont une pour le code. Les deux bandes ou puces restants représentent une valeur à débiter et une valeur à créditer. Les valeurs sur les puces sont modifiées par l'unité d'écriture du terminal. La carte magnétique sera débitée en cochant dans la bande de crédit et créditée en cochant dans la bande de débit. Elles fonctionnent comme les cartes de téléphones auxquelles on a ajouté des codes pour maintenir la sécurité des traitements.

Revendications.

1. Terminal intelligent pour traitement des cartes composé d'au moins une unité de lecture/écriture de cartes, d'un clavier, d'une unité centrale de traitement contenant un circuit de codage représentant au moins une partie d'une fonction non inversible, caractérisé en ce que la carte est authentifiée, ensuite testée grâce au circuit de codage, à son propre code et au mot de passe, et enfin traitée par débit et/ou crédit de ses valeurs seulement en cas de succès du test de validation.

2. Cartes à codes différents et non détectables en dehors du terminal selon la revendication 1, et ayant des valeurs modifiables par les terminaux de la revendication 1.