(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 749 956**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **96 08049**

(51) Int Cl[6] : **G 06 K 19/10**, G 06 F 17/60, G 07 C 9/00

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 28.06.96.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande :** 19.12.97 Bulletin 97/51.

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

(60) **Références à d'autres documents nationaux apparentés :** Division demandée le 28/06/96 bénéficiant de la date de dépôt du 19/04/96 de la demande initiale n° 96 04963

(71) **Demandeur(s) :** *LA POSTE* — FR.

(72) **Inventeur(s) :** GUERIN DIDIER, HARDY CONSTANT, GIRAULT MARC et REVILLET MARIE JOSEPHE.

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

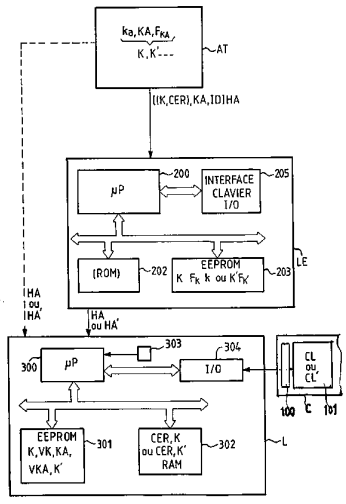
(74) **Mandataire :** CABINET BALLOT SCHMIT.

(54) SYSTEME SECURISE DE CONTROLE D'ACCES PERMETTANT LE TRANSFERT D'HABILITATION A PRODUIRE DES CLES.

(57) L'invention a pour objet un système de contrôle d'accès sécurisé au moyen d'un support de mémorisation portable (C) sur lequel est enregistrée une clé électronique (CL) des moyens de production (LE) de clés électroniques et un moyen assurant une fonction de serrure électronique (L) apte à autoriser l'accès dans le cas où le support de mémorisation comporte la clé électronique requise.

Selon l'invention, pour transférer une habilitation à produire des clés CL d'un moyen de production LE à un autre, on lui charge une nouvelle clé publique K' et la signature CER' de cette clé.

Application à la gestion des immeubles.



FR 2 749 956 - A1

SYSTEME SÉCURISÉ DE CONTROLE D'ACCES PERMETTANT LE TRANSFERT D'HABILITATION A PRODUIRE DES CLÉS.

La présente invention se rapporte à un système sécurisé de contrôle d'accès permettant le transfert d'habilitation à produire des clés.

L'invention s'applique tout particulièrement au domaine du contrôle d'accès à des bâtiments, à des systèmes informatiques ou à toutes sortes d'objets dont l'ouverture ou l'utilisation doit être contrôlée.

On connaît de la demande PCT/FR95/00935 publiée sous le numéro WO96/02899, un système de contrôle d'accès limités à des plages horaires autorisées et renouvelables.

Ce système repose sur l'utilisation de support de mémorisation portables tels que des cartes à puce (cartes à circuits intégrés) à contacts affleurants ou sans contacts, des cartes magnétiques, des badges des clés électroniques à contact ou sans contact. Ces supports sont distribués à tous les utilisateurs pour qui l'accès sera autorisé.

Pour cela, les supports de mémorisation possèdent en mémoire une clé électronique donnant un droit d'accès.

Cette clé comprend une donnée correspondant à une période d'autorisation d'accès et une signature numérique de cette donnée. La période d'utilisation correspond en pratique à une date d'utilisation et à une plage horaire d'utilisation si bien que la clé n'est valable que pendant un jour et pour la plage horaire définie.

Ces clés ont une durée de vie courte et sont particulièrement bien adaptées à une application telle que la distribution ou le ramassage du courrier par un

préposé. L'utilisateur d'un tel support doit tous le jours recharger son support avec une nouvelle clé valable.

Le problème du vol ou de la perte d'un support d'information comportant une telle clé ne se pose plus puisque la durée de vie de la clé logique est éphémère.

La personne qui a trouvé ou volé le support ne pourra plus l'utiliser le lendemain. Il n'est de ce fait même plus utile de tenir une liste noire de toutes les supports volés ou perdus.

Ce système de contrôle d'accès est très efficace dans des applications pour lesquelles on ne désire pas donner un droit d'accès permanent ou de très longue durée. En revanche, il s'avère ne pas être adapté dans le cas contraire.

Des systèmes de contrôle plus anciens proposent la tenue d'une liste noire pour les support volés ou perdus afin d'empêcher que les personnes non autorisées qui détiennent de tels supports ne puissent pas accéder à l'ensemble protégé.

La tenue de telles listes nécessite une intervention auprès des serrures électroniques. Il faut en effet enregistrer sur les serrures les numéros d'identification des supports volés ou perdus après que leur titulaire en ait fait la déclaration. Ces interventions sont contraignantes.

Dans le cas où une personne a une habilitation à produire des clés électroniques et à les enregistrer sur les supports de mémorisation, se voit retirer cette habilitation (dans le cas des droits d'accès à un immeuble, il s'agit par exemple du changement de syndic ou du gestionnaire de l'immeuble), le transfert d'habilitation à une autre personne, impose de donner à tous les utilisateurs qui avaient des droits d'accès,

de nouveaux supports sur lesquels les clés électroniques sont calculées avec le moyen de production de clé qui détient la nouvelle habilitation.

Ceci est une contrainte qui entraîne des frais importants.

Le système sécurisé de contrôle d'accès selon l'invention permet de résoudre ce problème, les supports délivrés restent toujours valables même en cas de transfert d'habilitation à une autre personne ou plus exactement à un autre moyen de production de clés.

L'invention à plus particulièrement pour objet un système de contrôle d'accès au moyen d'un support de mémorisation portable C sur lequel est enregistrée une clé électronique CL, des moyens de production LE de ces clés électroniques et un moyen assurant une fonction de serrure électronique L apte à autoriser l'accès dans le cas où le support de mémorisation comporte la clé électronique requise, selon lequel les moyens de production comportent une information d'habilitation HA à produire les clés CL, incluant une clé publique K, et la signature numérique CER de cette information, et dans lequel on opère un transfert d'habilitation à de nouveaux moyens de production en enregistrant une nouvelle clé publique K' et la signature correspondante CER'. Cette nouvelle clé publique est, après vérification de l'habilitation, enregistrée dans la serrure électronique L qui vérifie les clés CL produites par ces moyens LE.

Selon une autre caractéristique les données relatives aux moyens de production comportent une données d'identification ID, une durée de validité VAL et la clé publique K; la durée de validité affectée à l'ancienne clé K a une date de fin qui correspond à la

date de début de validité de la période de validité de la nouvelle clé K'.

Avantageusement, pour la vérification d'une nouvelle version de clé publique de signature CER', la serrure compare la date de début de période de validité de la nouvelle clé à la date de fin de validité de la clé précédente.

Les clés publiques K et K' sont obtenues par l'autorité à partir d'une fonction de production F_{KA} à clé publique KA, avec une clé secrète ka, la serrure comportant en mémoire au moment de la vérification une fonction de vérification V_{KA} et la clé KA pour la vérification de ces signatures CER ou CER'.

La serrure vérifie toute nouvelle habilitation.

Ainsi, lorsqu'un nouveau moyen de production est en service, ce moyen est déclaré auprès de la serrure qui va contrôler les clés produites par ce moyen.

Pour cela, l'autorité enregistre le certificat d'habilitation auprès de la serrure et la clé KA qu'elle a utilisé pour le calcul. Le moyen de production peut lui-même enregistrer son habilitation auprès de la serrure.

Les supports dont les clés ont été produites de manière frauduleuse par des moyens qui ne sont plus habilités, ne permettent pas l'accès aux ensembles protégés.

En effet, le transfert d'habilitation est réalisé par chargement sécurisé d'une nouvelle clé publique auprès de la serrure.

Les clés publiques précédentes sont en principe conservées à moins que l'algorithme de production ait été cassé ou la clé secrète du couple clé secrète, clé publique ait été découverte.

Selon une autre caractéristique, une signature électronique S est calculée à partir d'un algorithme à clé secrète k et d'une clé publique K correspondante par des moyens de production LE, la serrure possède en mémoire la clé publique K, une fonction de vérification V_K de cette signature S et des moyens pour mettre en oeuvre cette fonction de vérification.

La clé électronique CL enregistrée sur un support comporte une donnée d'identification de l'utilisateur et une donnée identifiant le support, on prendra par exemple pour cette donnée le numéro de série de fabrication du support et la signature électronique de ces données.

D'autres avantages et particularités de l'invention apparaîtront à la lecture de la description suivante qui est faite à titre indicatif et non limitatif et en regard du dessin de la figure 1 qui représente le schéma d' un système de contrôle d'accès sécurisé selon l'objet de l'invention.

Il est précisé que l'on entend par autorité un organisme possédant des clés secrètes, des moyens aptes à délivrer des clés publiques et des données d'habilitation.

On entend par clé secrète, une donnée numérique qui n'est connue que d'un organe de l'autorité ou le moyen de production.

On entend par clé publique KA, K, K' une donnée numérique partagée par plusieurs utilisateurs à savoir, l'autorité et les moyens de production des clés électroniques ou les moyens de production et la serrure électronique.

On entend par moyens de production LE de clés un appareil de traitement d'informations numériques, par exemple un microodinateur, détenant une information d'habilitation HA et ayant des moyens de calcul pour réaliser la signature numérique de données mettant en oeuvre des fonctions telles qu'un algorithme à clé publique classique.

On entend par clé électronique ou clé logique CL, une donnée numérique ou plusieurs données accompagnées de leur signature numérique donnant droit à un accès.

L'invention est décrite à titre d'exemple, dans l'application à la gestion d'accès à des immeubles.

On pourra se reporter au schéma de la figure 1 pour mieux comprendre.

Le support de mémorisation C comprenant les clés électroniques distribuées à des utilisateurs autorisés pourront être soit des cartes à puce, soit des clés à puce, soit des badges ou cartes magnétiques. La transmission entre le support C et la serrure L peut être faite à travers des contacts électroniques ou par des moyens radio-électriques ou par la lecture d'une bande magnétique.

A titre d'exemple, on a choisi comme support une carte à puce.

Elle comporte une interface d'entrée-sortie I/O 100 et une mémoire non volatile inscriptible électriquement 101.

Dans l'exemple décrit, la personnalisation d'un support C consiste en particulier à inscrire en mémoire une information d'identification IDA de l'utilisateur A comportant par exemple son nom, le numéro de son appartement et la donnée propre D_PA qui lui est affectée. Il s'agit selon un exemple préféré de

réalisation de la date de personnalisation de son support de mémorisation.

On inscrit aussi en mémoire une information identifiant le support, il s'agit par exemple du numéro de série NS de fabrication du support. En général, cette information est entrée à la fin de la fabrication, avant de remettre le support à l'autorité AT.

La personnalisation des supports est faite par l'appareil LE (et la personne qui l'utilise) qui détient une habilitation HA (ID, KA, CER, K).

L'appareil de production LE est par exemple réalisé par un microordinateur de type PC, muni d'un lecteur de cartes.

La figure 1, représente schématiquement les différents blocs fonctionnels de cet appareil LE.

L'appareil de production LE comporte une unité de traitement de type microprocesseur 200 relié par un bus 201 à des mémoires. Une mémoire volatile de travail de type RAM 202 contient les données de l'application.

Une mémoire non volatile de type EEPROM comporte en zone protégée la clé secrète k utilisée pour la production des clés électroniques. Elle comporte en outre le programme de production de clés électroniques. Ce programme met en oeuvre un algorithme de production de type algorithme à clé publique F_K utilisant la clé secrète k et la clé publique K correspondante.

La mémoire 203 comporte en outre le programme de personnalisation qui consiste à écrire la donnée propre, c'est-à-dire selon le mode préféré de réalisation la date D_PA du jour de personnalisation (plus l'heure éventuellement). Cette information est obtenue à partir d'une horloge interne.

La donnée propre peut également être obtenue par un compteur dont la valeur est augmentée (incrémentée de 1 par exemple) à chaque nouvelle version de clé.

L'exécution de ces programmes est lancée par la personne habilitée au moyen du clavier 205.

Selon un autre aspect de l'invention, la mémoire volatile 203, peut contenir également la clé publique KA et le certificat d'habilitation CER.

En effet, un appareil de production LE doit être habilité à produire des clés CL. L'habilitation lui est reprise par l'autorité AT.

En pratique, l'autorité lui donne une clé publique K qui va lui servir dans le calcul des clés CL. Cependant, la clé K lui est transmise avec une signature que l'on appelle ici certificat CER.

Ce certificat CER est donc la signature numérique d'un ensemble de données incluant l'identité de la personne habilitée ID, sa clé publique K et la période de validité VAL tel que :

$$CER = F_{KA}(ID, VAL, K),$$

F_{KA} étant l'algorithme à clé publique, ka étant la clé secrète de calcul du certificat et KA la clé publique correspondante. Ce calcul est fait par l'autorité AT.

Les serrures électroniques CL sont constituées par un appareil de type lecteur de cartes à puce ou microordinateur équipé d'une interface lecteur de cartes à puce pour l'exemple de réalisation décrit.

La serrure L comporte une unité de traitement 300, une mémoire non volatile 301 électriquement programmable et une mémoire de travail 302. La mémoire 301 comprend le programme de vérification des clés mettant en oeuvre une fonction de vérification V_K des clés électroniques CL.

Cette mémoire 301 contient également la clé publique K correspondant à la clé secrète k qui été utilisée pour la production des clés CL.

La serrure L permet de détecter de fausses clés électroniques.

Pour cela, la serrure compare la date de personnalisation D_PA de la clé CL à la date de personnalisation qu'elle a en mémoire pour le même support (identification IDA).

S'il y a égalité, la serrure autorise l'accès. Si la date D_PA > à la date de personnalisation présente dans la serrure, alors il s'agit d'une nouvelle version de clé, la serrure met à jour sa liste de clés, c'est-à-dire qu'elle enregistre la nouvelle à la place de l'ancienne.

S'il la date D_PA < à la date de personnalisation présente dans la serrure, alors il s'agit d'une réutilisation d'une clé déclarée volée ou perdue.

L'accès est interdit. Il n'y a pas de mise à jour de la liste des clés.

Lorsque l'on affecte une habilitation HA le couple clé publique et certificat CER de l'appareil LE de production des clés ainsi que la clé KA sont enregistrés dans la serrure en mémoire de travail par exemple, pour permettre à la serrure d'effectuer une vérification de l'habilitation.

Cette vérification est faite à chaque nouvelle habilitation. Pour cela la serrure contient aussi le programme de vérification du certificat, ce programme mettant en oeuvre une fonction de vérification V_{KA} du certificat. A l'issue de cette vérification, si le certificat correspond bien à la clé publique K la clé est enregistrée en mémoire EEPROM, le certificat et la clé KA ne sont pas conservés.

Lorsqu'un changement d'habilitation à lieu, un certificat CER' pour une nouvelle clé K' est calculé par l'autorité AT et chargé dans l'appareil LE tel que cela est illustré par le schéma de la figure 1.

Ainsi conformément à l'invention, ce changement d'habilitation consiste à utiliser une nouvelle clé publique K' et à affecter cette nouvelle clé K' à l'appareil.

Des clés électroniques CL calculées par l' appareil qui avaient l'ancienne clé publique K seront toujours valables ainsi que les nouvelles qui sont produites par un appareil qui a la clé K', dès l'instant où la serrure a vérifié cette nouvelle habilitation.

On choisit la durée de validité affectée à la clé K pour qu'elle ait une date de fin de validité égale à la date de début de la période de validité affectée à la clé K' ou une date légèrement postérieure (un mois par exemple).

Dans le cas où un appareil de production LE a une donnée d'habilitation HA (ID, KA, CER, K) qu'il s'agisse d'une première habilitation ou d'une nouvelle habilitation, et dans le cas où les clé produites CL (S, D_pA, IDA) ont une donnée propre telle que la date de personnalisation du support sur lequel elles sont enregistrées, la serrure pourra vérifier les conditions d'accès énoncées dans la première partie de la description et en outre comparer la date D_pA à la période de validité de la clé publique de l'appareil.

Cette comparaison va permettre par exemple de déceler les clés CL qui auraient été produites alors que l'appareil de production LE n'avait plus l'habilitation.

En effet, les dates de personnalisations DpA tombent obligatoirement soit dans l'une, soit dans

l'autre des périodes de validité VAL ou VAL' des clés K ou K'.

Dans chaque cas, la serrure pourra alors comparer la date de personnalisation à la période de validité correspondant à la clé publique correspondante. La serrure autorise l'accès lorsque, à l'issue de cette vérification, elle trouve que la date D_pA est à l'intérieur de la période de validité de la clé publique correspondante.

Comme chaque clé publique K ou K' a une période de validité qui lui est propre, il est facile de détecter la fraude.

REVENDICATIONS

1. Système de contrôle d'accès au moyen d'un support de mémorisation portable (C) sur lequel est enregistré une clé électronique CL, des moyens de production (LE) des clés électroniques et un moyen assurant une fonction de serrure électronique (L) apte à autoriser l'accès dans le cas où le support de mémorisation comporte la clé électronique requise, caractérisé en ce que les moyens de production (LE) comportent une information d'habilitation (HA) à produire les clés CL, incluant une clé publique (K), et la signature numérique CER de cette clé, et en ce que l'on opère un transfert d'habilitation à de nouveaux moyens de productions en enregistrant une nouvelle clé publique K' et la signature correspondante CER'.

2. Système de contrôle d'accès selon la revendication 1, caractérisé en ce que l'information d'habilitation comporte une donnée d'identification (ID), une durée de validité VAL et la clé publique K, et en ce que la durée de validité affectée à l'ancienne clé K a une date de fin qui correspond à la date de début de validité de la période de validité de la nouvelle clé K', cette date pouvant lui être postérieure.

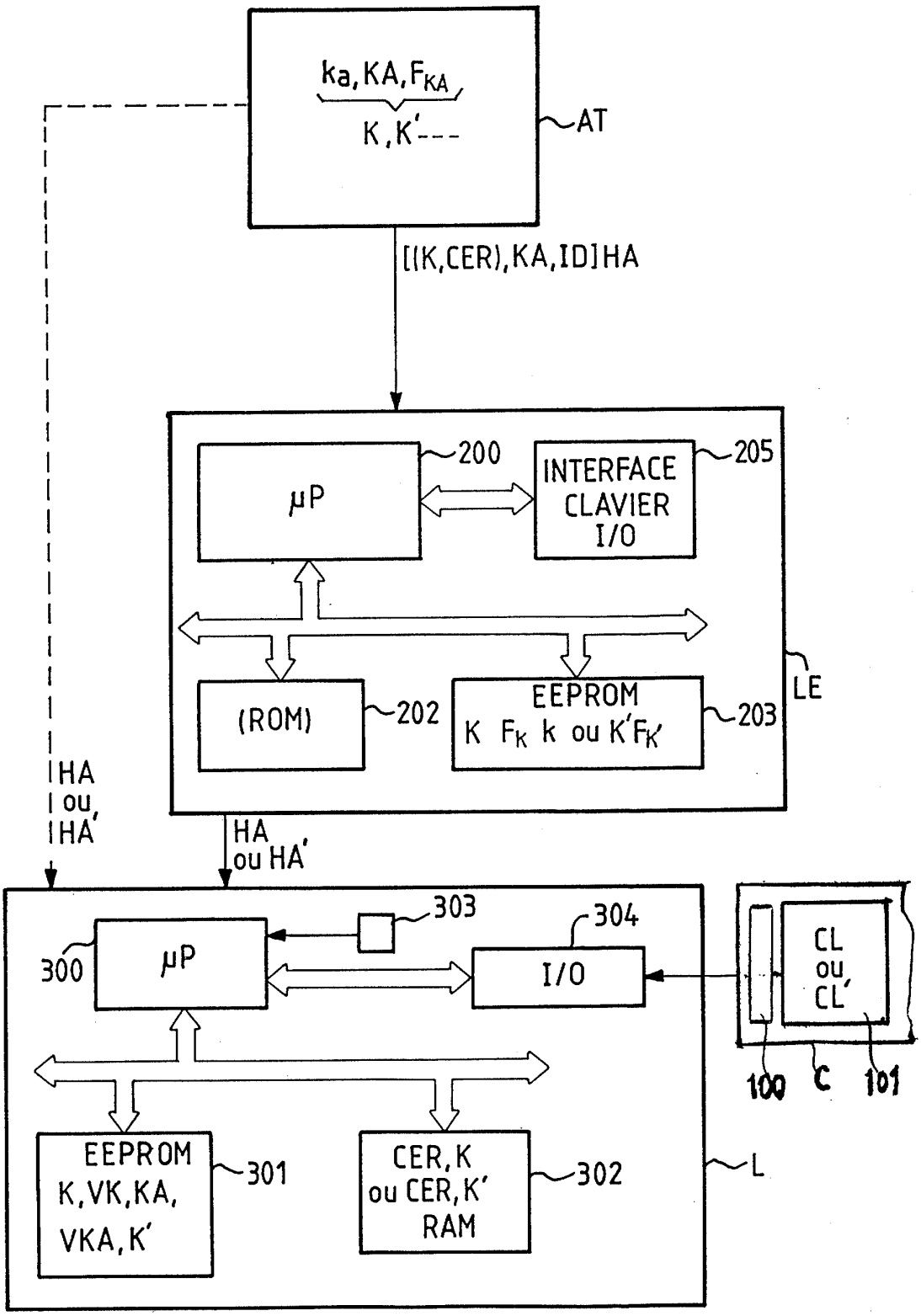
3. Système de contrôle d'accès selon la revendication 1 et 2, caractérisé en ce que pour la vérification d'une nouvelle version de clé K' de signature CER', la serrure utilise une fonction de vérification à clé publique, en outre la serrure compare la date de début de période de validité de la

nouvelle clé à la date de fin de validité de la clé précédente.

4. Système de contrôle d'accès selon l'une quelconque des revendications précédentes 1 à 3, caractérisé en ce que les clés sont obtenues par l'autorité (AT) à partir d'une fonction de production F_{KA} à clé publique KA, la serrure comportant en mémoire au moment de la vérification une fonction de vérification V_{KA} et la clé KA.

1 / 1

FIG_1


ka, KA, F_{KA}
K, K'---
AT
[(K,CER),KA,ID]HA
µP
200
INTERFACE CLAVIER I/O
205
(ROM)
202
EEPROM
K F_K k ou K'$F_{K'}$
203
LE
HA ou HA'
HA ou HA'
303
304
300
µP
I/O
CL ou CL'
100
C
101
EEPROM
K,VK,KA,
VKA,K'
301
CER,K
ou CER,K'
RAM
302
L

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

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

2749956
N° d'enregistrement national

FA 530403
FR 9608049

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
A	FR 2 531 128 A (GENEST) * page 10, ligne 10 - ligne 23; figures 1,2 *	1,2
A	FR 2 597 142 A (SCHLAGE LOCK COMPANY) * page 6, ligne 23 - page 8, ligne 16; figures 4,5 *	1,4
D,A	WO 96 02899 A (GIRAULT,REITTER,REVILLET) * page 9, ligne 12 - page 11, ligne 13; figure 1 *	1,4

DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)

G07C
G07F

Date d'achèvement de la recherche	Examinateur
10 Janvier 1997	Herbelet, J.C.

CATEGORIE DES DOCUMENTS CITES

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

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

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)