PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets[4] :		(11) Numéro de publication internationale: WO 88/ 00744
G07F 7/10	A1	(43) Date de publication internationale: 28 janvier 1988 (28.01.88)

(21) Numéro de la demande internationale: PCT/FR87/00273

(22) Date de dépôt international: 9 juillet 1987 (09.07.87)

(31) Numéro de la demande prioritaire: 86/10416

(32) Date de priorité: 17 juillet 1986 (17.07.86)

(33) Pays de priorité: FR

(71) Déposant *(JP seulement):* BULL CP8 [FR/FR]; Rue Eugène Hénaff, F-78190 Trappes (FR).

(72) Inventeur; et
(75) Inventeur/Déposant *(US seulement) :* HAZARD, Michel [FR/FR]; 27, rue des Harias, F-78124 Mareil/Mauldre (FR).

(74) Mandataire: DEBAY, Yves; Bull S.A., 25, avenue de la Grande Armée, F-75016 Paris (FR).

(81) Etats désignés: JP, US.

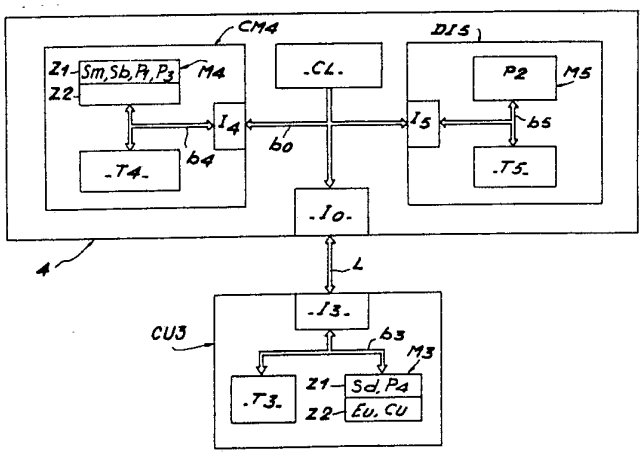
Publiée
Avec rapport de recherche internationale.

(54) Title: PROCESS FOR DIVERSIFYING A BASIC KEY AND FOR AUTHENTICATING A THUS DIVERSIFIED KEY AS HAVING BEEN PREPARED FROM A PREDETERMINED BASIC KEY, AND SYSTEM FOR ITS IMPLEMENTATION

(54) Titre: PROCEDE POUR DIVERSIFIER UNE CLE DE BASE ET POUR AUTHENTIFIER UNE CLE AINSI DIVERSIFIEE COMME AYANT ETE ELABOREE A PARTIR D'UNE CLE DE BASE PREDETERMINEE, ET SYSTEME POUR LA MISE EN ŒUVRE

(57) Abstract

An initialization system calculates a diversified key (Sd) from a basic key (Sb) processed by a one-two-one combinational transformation (T). The key (Sd) recorded in the memory (M3) of a user card (CU3) is authenticated by an operating system (4) which calculates a certificate from the basic key (Sb), whereas the card (CU3) calculates a certificate from its key (Sd). This certificate must be identical taking into account the characteristics of the transformation (T). The invention is applicable in particular to secret keys recorded in memory cards.



(57) Abrégé

Un système d'initialisation calcule une clé diversifiée (Sd) à partir d'une clé de base (Sb) traitée par une transformation combinatoire biunivoque (T). La clé (Sd) enregistrée dans la mémoire (M3) d'une carte usager (CU3) est authentifiée par un système d'exploitation (4) qui calcule un certificat à partir de la clé de base (Sb), alors que la carte (CU3) calcule un certificat à partir de sa clé (Sd). Ces certificats doivent être identiques compte tenu des propriétés de la transformation (T). L'invention s'applique notamment aux clés secrètes enregistrées dans les cartes à mémoire.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AT	Autriche	**FR**	France	**ML**	Mali
AU	Australie	**GA**	Gabon	**MR**	Mauritanie
BB	Barbade	**GB**	Royaume-Uni	**MW**	Malawi
BE	Belgique	**HU**	Hongrie	**NL**	Pays-Bas
BG	Bulgarie	**IT**	Italie	**NO**	Norvège
BJ	Bénin	**JP**	Japon	**RO**	Roumanie
BR	Brésil	**KP**	République populaire démocratique de Corée	**SD**	Soudan
CF	République Centrafricaine			**SE**	Suède
CG	Congo	**KR**	République de Corée	**SN**	Sénégal
CH	Suisse	**LI**	Liechtenstein	**SU**	Union soviétique
CM	Cameroun	**LK**	Sri Lanka	**TD**	Tchad
DE	Allemagne, République fédérale d'	**LU**	Luxembourg	**TG**	Togo
DK	Danemark	**MC**	Monaco	**US**	Etats-Unis d'Amérique
FI	Finlande	**MG**	Madagascar		

Procédé pour diversifier une clé de base et pour authentifier une clé ainsi diversifiée comme ayant été élaborée à partir d'une clé de base prédéterminée, et système pour la mise en oeuvre.

L'invention a pour objet un procédé pour diversifier une clé de base et pour authentifier une clé ainsi diversifiée comme ayant été élaborée à partir d'une clé de base prédéterminée, et un système pour la mise en oeuvre du procédé.

Un tel procédé permet notamment de diversifier les clés secrètes enregistrées dans des supports portatifs tels que des cartes à mémoire.

L'essor des applications qui mettent en oeuvre des objets portatifs tels que des cartes est essentiellement dû à l'avénement des cartes à mémoire dont une caractéristique essentielle est de posséder des circuits de traitement. Ces circuits comprennent généralement un microprocesseur qui effectue des calculs non seulement sur des données entrées de l'extérieur, mais surtout sur des données internes inaccessibles de l'extérieur.

De telles cartes sont distribuées à des utilisateurs par des organismes habilités qui proposent la délivrance de services par l'intermédiaire d'appareils ou terminaux mis à la disposition du public et auxquels l'utilisateur accouple temporairement sa carte.

Tout appareil ne délivre généralement le service demandé qu'après s'être préalablement assuré que la carte a bien été établie à l'origine comme pouvant donner accès à ce service.

En effet, il faut éviter à tout prix qu'une carte établie pour accéder à un service (A) ne puisse être également utilisée pour accéder à un service (B), ou qu'un fraudeur ne puisse concevoir ou simuler une fausse carte donnant accès au service (A) et/ou (B).

Ces buts sont généralement atteints par l'établissement préalable d'un échange d'informations sous forme d'un dialogue entre la carte et l'appareil.

Un type de dialogue tel que décrit dans le brevet américain N° 4 471 216 de la demanderesse correspondant à son brevet français N° 2 469 760 prend en compte une clé secrète seule connue de l'organisme habilité et enregistrée à la fois dans la carte et dans l'appareil. A titre d'exemple, la carte calcule un résultat qui est fonction de sa clé secrète et l'appareil calcule un résultat similaire qui est fonction de sa clé secrète. Les résultats sont comparés par l'appareil qui n'autorisera l'accès au service demandé qu'en cas d'identité ou de concordance entre ces résultats. Cette condition ne peut être satisfaite que si les clés de la carte et de l'appareil sont identiques.

Ainsi, tout appareil conçu pour délivrer un service donné est apte à reconnaître l'ensemble des cartes qui auront été délivrées par un organisme habilité pour obtenir l'accès à ce service.

Cependant, pour une même clé secrète enregistrée dans un appareil, il y a n cartes d'une même famille possédant cette clé secrète (n pouvant atteindre plusieurs millions, notamment dans les applications bancaires). Si un fraudeur parvient à percer le secret de cette clé, il se trouve dans la possibilité de pouvoir fabriquer et diffuser de fausses cartes qui seront cependant reconnues comme

valables par les appareils. Une telle conséquence serait donc catastrophique et nécéssiterait le changement de la clé secrète et la distribution de nouvelles cartes.

Pour pallier cet inconvénient, l'invention prévoit de diversifier les clés secrètes des cartes à partir d'une même clé de base tout en permettant aux appareils de les reconnaître comme ayant été élaborées à partir d'une même clé de base. Ainsi, chaque carte aura une clé secrète propre et différente des clés attribuées aux autres cartes.

L'invention propose donc un procédé pour diversifier une clé de base par un système d'initialisation, chaque clé de base ainsi diversifiée étant enregistrée dans une mémoire d'un dispositif objet, et pour faire reconnaître par un système d'exploitation que la clé diversifiée enregistrée dans un dispositif objet a bien été élaborée à partir d'une clé de base prédéterminée, caractérisé en ce qu'il consiste :

- pour diversifier une clé de base (Sb) préenregistrée dans une mémoire du système d'initialisation, à faire calculer par des circuits de traitement de ce système une clé diversifiée (Sd) telle que :

$$Sd = Du\ (T)\ Sb$$

où (Du) est un paramètre de diversification propre à chaque dispositif objet et (T) une transformation combinatoire biunivoque, et à enregistrer cette clé (Sd) dans la mémoire du dispositif objet,

- et pour faire reconnaître la clé diversifiée (Sd) d'un dispositif objet comme ayant été élaborée à partir d'une clé de base (Sb), à accoupler le dispositif objet avec un

système d'exploitation ayant une mémoire où est enregistrée la clé de base (Sb), à faire calculer par des circuits de traitement de ce système un paramètre intermédiaire (Pu) tel que :

$$Pu = Cu\ (T)\ Du$$

où (Cu) est une donné propre à chaque dispositif objet, (T) la transformation précitée et (Du) le paramètre de diversification précité,

et à faire calculer d'une part par le système d'exploitation un certificat (R1) tel que :

$$R1 = f3\ (K1, Ex)$$

avec $K1 = Sb\ (T)\ Pu)$

où (Ex) est une information externe, et d'autre part par le dispositif objet un certificat (R2) tel que :

$$R2 = f4\ (K2, Ex)$$

avec $K2 = Sd\ (T)\ Cu$

ces deux certificats étant identiques si la clé diversifiée (Sd) du dispositif objet a bien été calculée à partir de la même clé de base (Sb) que celle enregistrée dans le système d'exploitation (4).

Selon une caractéristique du procédé, la transformation (T) est une fonction OU exclusif.

D'autres avantages, caractéristiques et détails apparaîtront à la lumière de la description explicative qui va suivre faite en référence aux dessins annexés donnés à titre d'exemple :

- la figure 1 montre schématiquement un système d'initialisation pour illustrer la première phase du procédé conforme à l'invention,

- et la figure 2 montre schématiquement un système d'exploitation pour illustrer la deuxième phase du procédé conforme à l'invention,

D'une façon générale, le procédé conforme à l'invention se décompose en une phase d'initialisation et en une phase d'exploitation.

La phase d'initialisation consiste :

- à faire calculer par un système d'initialisation une clé diversifiée à partir d'une clé de base prédéterminée,

- et à enregistrer cette clé secrète ainsi diversifiée dans une mémoire d'un objet portatif.

Cette première phase est réalisée par un organisme habilité qui remet ensuite l'objet portatif à un utilisateur, chaque objet portatif ayant une clé secrète différente. Chaque utilisateur pourra ensuite demander l'accès à des services au moyen de son objet portatif, mais ces accès ne pourront être validés qu'après un contrôle basé sur la reconnaissance de la clé diversifiée enregistrée dans l'objet portatif. Ce contrôle fait l'objet de la deuxième phase ou phase d'exploitation qui sera décrite plus loin.

Le système d'initialisation (1) représenté à la figure 1 se compose notamment d'un dispositif source (CM1), d'un dispositif intermédiaire (DI2), d'un dispositif d'entrée tel qu'un clavier (CL) et d'une interface d'entrée-sortie (IO).

Le dispositif source (CM1) se compose notamment d'une mémoire (M1), de circuits de traitement (T1) tels qu'un microprocesseur, et d'une interface d'entrée/sortie (I1). L'ensemble de ces circuits sont reliés entre eux par un bus de liaison (b1).

Dans la mémoire (M1) du dispositif source (CM1) sont au moins enregistrées les informations suivantes :

- une clé secrète intermédiaire (Sm),

- et un programme de calcul (P1) dont la fonction sera explicitée plus loin.

Le dispositif intermédiaire (DI2) se compose notamment d'une mémoire (M2), de circuits de traitement (T2) tels qu'u microprocesseur et d'une interface d'entrée-sortie (I2). L'ensemble de ces circuits sont reliés entre eux par une bus de liaison (b2).

La mémoire (M2) du dispositif intermédiaire (DI2) contient les informations suivantes :

- une clé de base prédéterminée (Sb), - et un programme (P2) dont la fonction sera explicitée plus loin.

Les interfaces (I1, I2) du dispositif source (CM1) et du dispositif intermédiaire (DI2) sont reliées ensemble ainsi que le clavier (CL) et l'interface d'initialisation (1) par un bus de liaison (b0).

Un objet portatif (CU3) à initialiser se compose notamment d'une mémoire (M3), de circuits de traitement (T3) tels qu'un microprocesseur et d'une interface d'entrée-sortie (I3). L'ensemble de ces circuits sont reliés par un bus de liaisons (b3).

Selon un mode préférentiel de réalisation, l'objet portatif (CU3) ou carte usager est constitué par une carte à mémoire telle celle décrite dans les brevets américains N° 4 211 919 et 4 382 279 correspondant respectivement aux brevets français n° 2 401 459 et 2 461 301 de la demanderesse.

La carte usager (CU3) est accouplée au système d'initialisation par une ligne de transmission (L) qui relie les interfaces (I0, I3). Une telle ligne (L) est notamment décrite dans le brevet américain N° 4 556 958 correspondant au brevet français n° 2 483 713 de la demanderesse.

Le système d'initialisation (1) a donc pour fonction de calculer une clé diversifiée (Sd) à partir d'une clé de base prédéterminée (Sb).

Le principe de ce calcul est le suivant. Dans un premier temps, on calcule un paramètre de diversification (Du) à partir de données spécifiques à chaque carte usager à initialiser et d'une clé de base intermédiaire (Sm). Dans un deuxième temps, on calcule la clé diversifiée (Sd) à partir du paramètre de diversification (Du) et de la clé de base prédéterminée (Sb).

Dans un premier mode de réalisation, le calcul du paramètre de diversification (Du) est effectué par le dispositif source (CM1) et le calcul de la clé diversifiée (Sd) est effectué par le dispositif intermédiaire (DI2).

Plus précisément, les circuits de traitement (T1) du dispositif source (CM1) exécutent le programme (P1) précité pour calculer un paramètre de diversification (Du) tel que :

$$Du = f1 (Sm, Eu, Cu)$$

où (Sm) est la clé de base intermédiaire précitée enregistrée dans la mémoire (M1), (Eu) est une donnée spécifique de la carte usager (CU3) entrée au clavier (CL) et enregistrée dans la mémoire (M3), et (Cu) une donnée de diversification spécifique de la carte usager (CU3) soit externe et entrée au clavier(CL) avant d'être enregistrée dans la mémoire (M3), soit interne et déjà préenregistrée dans la mémoire (M3).

Ensuite, le dispositif intermédiaire (DI2) calcule une clé diversifiée (Sd) à partir de la clé de base prédéterminée (Sb) enregistrée dans sa mémoire (M2) et du paramètre de diversification (Du) calculé par le dispositif source (CM1) et transmis par le bus (b0) au dispositif intermédiaire (DI2).

La clé diversifiée (Sd) est calculée par les circuits de traitement (T2) qui exécutent le programme (P2) qui est la mise en oeuvre d'une transformation combinatoire biunivoque (T) telle que :

$$Sd = Sb (T) Du$$

A titre d'exemple, cette transformation est une fonction OU EXCLUSIF.

Enfin, la clé diversifiée (Sd) ainsi calculée est enregistrée dans la mémoire (M3) de la carte (CU3).

Il est à noter que la mémoire (M3) de la carte usager (CU3) est avantageusement divisée en au moins deux zones (Z1, Z2). La zone de mémoire (Z1) est telle que les informations une fois enregistrées sont inaccessibles depuis l'extérieur, mais uniquement accessibles par les

circuits de traitement (T3). La zone de mémoire (Z2) est telle que les informations enregistrées peuvent être lues mais non modifiées depuis l'extérieur. De tels accès mémoire sont notamment décrit dansle brevet américain N° 4 211 919 de la demanderesse correspondant à son brevet français n° 2 401 459.

Comme la zone de mémoire (Z1) permet de préserver le secret des informations enregistrées, la clé diversifiée (Sd) est enregistrée dans cette zone, alors que les données (Eu, Cu) propres à l'usager sont enregistrées dans la zone (Z2).

La phase d'initialisation ainsi décrite est généralement complétée par l'écriture dans la mémoire (M3) de la carte (CU3) de plusieurs autres informations spécifiques de chaque application.

Une carte usager ainsi initialisée par un organisme habilité est remise à un utilisateur qui peut ensuite obtenir la délivrance d'un service auquel donne droit sa carte en l'accouplant à un appareil ou terminal chargé de cette délivrance et géré par l'organisme habilité.

Avant d'assurer cette délivrance, l'appareil doit s'assurer que la carte présentée possède une clé secrète authentique, c'est-à-dire que cette clé a bien été calculée à partir de la clé de base qui est propre au service demandé et préenregistrée dans tout l'appareil chargé de dispenser ce service. Dans le cas contraire, l'appareil aura détecté soit une fausse carte, soit une bonne carte mais qui n'aura pas été initialisée pour obtenir la délivrance du service dispensé par cet appareil.

Ce contrôle fait l'objet de la deuxième phase du procédé ou phase d'exploitation telle que décrite en référence à la figure 2.

Le système d'exploitation (4) est composé d'un dispositif de contrôle (CM4), d'un disposisitif intermémdiaire (DI5), d'un dispositif d'entrée (CL) tel qu'un clavier par exemple et d'une interface d'entrée-sortie (I0).

Le dispositif de contrôle (CM4) se compose notamment d'une mémoire (M4), de circuits de traitement (T4) tels qu'un microprocesseur, et d'une interface d'entrée-sortie (I4). L'ensemble de ces circuits sont reliés entre eux par un bus de liaison (b4).

Dans la mémoire (M4) sont au moins enregistrées les informations suivantes :

- les clés secrètes (Sm, Sb) utilisées lors de la phase d'initialisation,
- le programme (P1) également utilisé dans la phase d'initialisation pour calculer le paramètre de diversification (Du),
- et un programme (P3) dont la fonction sera explicitée plus loin.

Le dispositif intermédiaire (DI5) se compose notamment d'une mémoire (M5), de circuits de traitement (T5) tels qu'un microproceseur, et d'une interface d'entrée-sortie (I5). L'ensemble de ces circuits sont reliés entre eux par un bus de liaison (b5).

La mémoire (M5) du dispositif intermédiaire (DI5) contient au moins le même programme (P2) dont la fonction sera explicitée plus loin.

Les interfaces (I4, I5) du dispositif de contrôle (CM4) et du dispositif intermédiaire (DI5) sont reliées ensemble ainsi qu'au clavier (CL) et à l'interface (I0) du système d'exploitation (4) par un bus de liaison (b0).

Soit une carte usager (CU3) telle que précédemment initialisée et accouplée temporairement au système d'exploitation (4). Cet accouplement est obtenu par une ligne de transmission (L) du type précité qui relie l'interface (I0) du système (4) et l'interface (I3) de la carte (CU3).

Dans un premier temps, le dispositif de contrôle (CM4) recalcule un paramètre de diversification (Du) par exécution du programme (P1) par les circuits de taitement (T4). Ce paramètre (Du) est tel que :

$$Du = f1\ (Sm, Eu, Cu)$$

où les paramètres (Eu, Cu) ont été prélevés de la mémoire (M3) de la carte usager (CU3).

Une fois calculé, le paramètre de diversification est transmis au dispositif intermédiaire (DI5) dont les circuits de traitement (T5) vont exécuter le programme (P2) pour obtenir un paramètre (Pu) tel que :

$$Pu = Du\ (T)\ Cu$$

où (Cu) est le paramètre prélevé de la mémoire (M3) de la carte usager (CU3).

A ce stade du procédé, il est important de noter une originalité de l'invention. Le dispositif de contrôle (CM4) et le dispositif intermédiaire (DI5) ne recalculent pas directement une clé diversifiée (Sd) à partir de la clé de base (Sb) pour la comparer ensuite à celle enregistrée dans la carte usager (CU3). Ainsi, la clé diversifiée (Sd) est d'autant mieux protégée.

Pour permettre cependant une reconnaissance de la clé diversifiée (Sd) enregistrée dans la carte usager (CU3),

le dispositif de contrôle (CM4) et la carte (CU3) vont respectivement calculer le résultat dénommé certificat. Ces certificats seront identiques si la clé diversifiée (Sd) de la carte (CU3) a été calculée à partir de la même clé de base (Sb) que celle enregistrée dans la mémoire (M4) du dispostif de contrôle (CM4). L'identité des deux certificats est basée sur les relations qui existent entre les clés secrètes (Sb, Sd) et les paramètres (Pu, Du) comme explicité ci-après.

Un premier certificat ou résultat (R1) est calculé par les circuits de traitement (T4) du dispositif de contrôle (CM4) par exécution du programme (P3) enregistré dans la mémoire (M4). Ce résultat (R1) est tel que :

$$R1 = f3\ (K1,\ Ex)$$

$$\text{avec} \quad K1 = Sb\ (T)\ Pu$$

où (Sb) est la clé de base enregistrée dans a mémoire (M4), (Pu) le paramètre calculé par le dispositif intermédiaire (DI5), et (Ex) une donnée externe entrée par exemple au clavier (CL) par un opérateur ou par l'usager.

De leur côté, les circuits de traitement (T3) de la carte usager (CU3) exécutent le programme (P4) préenregistré dans la mémoire (M3) lors de la phase d'initialisation pour obtenir un second certificat ou résultat (R2) tel que :

$$R2 = f4\ (K2,\ Ex)$$

$$\text{avec} \quad K2 = Sd\ (T)\ Cu$$

où (Sd) est la clé diversifiée enregistrée dans la mémoire (M3), (Cu) le paramètre prélevé dans la zone de mémoire (Z2), et (Ex) la donnée externe précitée.

Si la clé diversifiée (Sd) a bien été calculée à partir d'une clé de base (Sb) identique à celle enregistrée dans le dispositif de contrôle (CM4), les deux résultats (R1, R2) seront identiques pour les raisons suivantes :

- le paramètre intermédiaire (K2) pour le calcul du résultat (R2) est tel que :

$$K2 = Sd\ (T)\ Cu$$

or : $Sd = Sb\ (T)\ Du$

d'où : $K2 = Sb\ (T)\ Du\ (T)\ Cu$

or : $Pu = Cu\ (T)\ Du$

d'où : $K2 = Sb\ (T)\ Pu = K1$ (paramètre intermédiaire utilisé pour le calcul du résultat (R1).

Toutes ces égalités sont satisfaites car la transformation (T) utilisée est une transformation commutative.

Bien entendu, si au moins l'une de ces égalités n'est pas satisfaite, la clé diversifiée (Sd) du dispositif objet (CU3) n'est pas reconnue comme authentique et le dialogue est interrompu.

Il ressort de ce qui prècède que le dispositif source (CM1) et le dispositif intermédiaire (DI2) du système d'initialisation (1), ainsi que le dispositif de contrôle (CM4) et le dispositif intermédiaire (DI5) du système d'exploitation (4), renferment des informations qui doivent rester secrètes pour interdire la fraude qui peut consister à simuler de fausses cartes usagers (CU3) qui soient reconnues comme authentiques par le dispositif de contrôle (CM4).

Il est donc indispensable de prendre des mesures de sécurité pour protéger l'accès aux informations contenues dans les mémoires (M1, M2, M4 et M5).

Une première solution consiste à prendre des mesures de protection physiques ou matérielles rendant difficilement accessibles ces mémoires.

Une deuxième solution consiste, une fois les informations écrites, à verrouiller les accès mémoire de manière à les rendre inaccessibles de l'extérieur, mais uniquement accessibles par les circuits de traitement respectivement associés à ces mémoires.

Cette deuxième solution est satisfaite si les mémoires correspondent aux mémoires d'objets portatifs tels que les cartes usagers (CU3). Plus présisément, la mémoire (M1) et les circuits de traitement (T1) du dispositif source (CM1) du système d'initialisation (1) d'une part, et la mémoire (M4) et les circuits de traitement (T4) du dispositif de contrôle (CM4) du système d'exploitation (4) d'autre part, sont intégrés dans une carte du type usager où chaque mémoire (M1, M4) est divisée en aù moins deux zones de mémoire (Z1, Z2).

Une troisième solution consiste à regrouper le dispositif source (CM1) et le dispositif intermédiaire (DI2) du système d'initailisation (1) dans un même dispositif conçu par exemple sous la forme d'un boîtier à circuits intégrés avec les mêmes caractéristiques d'accès à la mémoire qu'une carte précitée. Cette solution s'applique également au dispositif de contrôle (CM4) et au dispositif intermédiaire (DI5) du système d'exploitation (4).

En variante de cette troisième solution, le boîtier à circuits intégrés précité est inclus dans un objet portatif et notamment dans une carte à mémoire précitée.

Revendications :

1. Procédé pour diversifier une clé de base par un système d'initialisation, chaque clé diversifiée étant enregistrée dans une mémoire d'un dispositif objet, et pour faire reconnaître par un système d'exploitation que le clé diversifiée d'un dispositif objet a bien été élaborée à partir d'une clé de base prédéterminée, caractérisé en ce qu'il consiste :

- pour diversifier une clé de base (Sb) préenregistrée dans une mémoire (M2) du système d'initialisation (1), à faire calculer par des circuits de traitement (T1, T2) de ce système (1) une clé diversifiée (Sd) telle que :

$$Sd = Du\ (T)\ Sb$$

où (Du) est un paramètre de diversification propre à chaque dispositif objet (CU3) et (T) une transformation combinatoire biunivoque, et à enregistrer cette clé (Sd) dans la mémoire (M3) du dispositif objet (CU3),

- et pour faire reconnaître la clé diversifiée (Sd) d'un dispositif objet (CU3) comme ayant été élaborée à partir d'une clé base (Sb), à accoupler le dispositif objet (CU3) avec un système d'exploitation (4) ayant une mémoire (M4) où est enregistrée la clé de base (Sb), à faire calculer par des circuits de traitement (T4, T5) de ce système (4) un paramètre intermédiaire (Pu) tel que :

$$Pu = Cu\ (T)\ Du$$

où (Cu) est une donnée propre à chaque dispositif objet (CU3), (T) la transformation précitée et (Du) le paramètre de diversification précité,

et à faire calculer d'une part par le système d'exploitation (4) un certificat (R1) tel que :

$$R1 = f3\ (K1,\ Ex)$$

avec $K1 = Sb\ (T)\ Pu$

où (Ex) est une information externe, et d'autre part par le dispositif objet (CU3) un certificat (R2) tel que :

$$R2 = f4\ (K2,\ Ex)$$

avec $K2 = Sd\ (T)\ Cu$

ces deux certificats (R1, R2) étant identiques si la clé diversifiée (Sd) du dispositif objet (CU3) a bien été calculée à partir de la même clé de base (Sb) que celle enregistrée dans le système d'exploitation (4).

2. Procédé selon la revendication 1, caractérisé en ce qu'il consiste à faire calculer par le système d'initialisation (1) le paramètre de diversification (Du) précité par exécution d'un programme (P1) enregistré dans sa mémoire (M1) et qui prend en compte une donnée (Eu) propre au dispositif objet (CU3).

3. Procédé selon la revendication 2, caractérisé en ce que le programme (P1) précité prend également en compte une clé intermédiaire (Sm) préenregistrée dans la mémoire (M1) du système d'initialisation (1).

4. Procédé selon la revendication 1, caractérisé en ce qu'il consiste à faire calculer par le système d'exploitation (4) le paramètre de diversification (Du) précité par exécution d'un programme (P1) enregistré dans sa mémoire (M4) et qui prend en compte une donnée (Eu) propre au dispositif objet (CU3).

5. Procédé selon la revendication 4, caractérisé en ce que le programme (P1) précité prend également en compte une clé intermédiaire (Sm) préenregistrée dans la mémoire (M4) du système d'exploitation (4).

6. Procédé selon la revendication (1) caractérisé en ce qu'il consiste à prendre pour la transformation (T) précitée une fonction OU EXCLUSIF.

7. Système d'initialisation pour la mise en oeuvre du procédé tel que défini selon l'une des revendications 1 à 6, caractérisé en ce qu'il comprend pour initialiser un dispositif objet (CU3) avec une clé diversifiée (Sd) :

- des moyens d'accouplement (I0, I3, L) avec le dispositif objet (CU3), - une mémoire (M2) ou est enregistrée une clé de base (Sb) et un programme (P2), - des circuits de traitement (T2) pour calculer la clé diversifiée (Sd) par exécution du programmme (P2) qui est la mise en oeuvre d'une transformation (T) combinatoire biunivoque, et telle que :

$$Sd = Sb\ (T)\ Du$$

où (Du) est un paramètre de diversification propre à chaque dispositif objet (CU3).

8. Système selon la revendication 7, caractérisé en ce qu'il comprend également des circuits de traitement (T1) pour calculer le paramètre de diversification (Du) précité par exécution d'un programme (P1) enregistré dans une mémoire (M1) et qui prend en compte au moins une donnée (Eu) propre au dispsositif objet (CU3).

9. Système selon la revendication 8, caractérisé en ce que le programme (P1) précité prend également en compte une clé intermédiaire (Sm) préenregistrée dans la mémoire (M1).

10. Système selon l'une des revendications 7 à 9, caractérisé en ce que les circuits de traitement (T1) et la mémoire (M1) précitée sont intégrés dans un objet portatif tel qu'une carte à mémoire (CM1).

11. Système selon l'une des revendications 7 à 9, caractérisé en ce que les circuits de traitement (T1, T2) et les mémoires (M1, M2) sont intégrés dans un boîtier à circuits intégrés.

12. Système selon la revendication 11, caractérisé en ce que le boîtier précité est logé dans un objet portatif tel qu'une carte à mémoire.

13. Système d'exploitation pour la mise en oeuvre du procédé tel que défini selon l'une des revendications 1 à 6, caractérisé en ce qu'il comprend pour reconnaître la clé diversifiée (Sd) enregistrée dans un dispositif objet (CU3) :

- des moyens d'accouplement (I0, I3, L) avec le dispositif objet (CU3),

- une mémoire (M5) où est enregistrée un programme (P2) et des circuits de traitement (T5) pour calculer un paramètre intermédiaire (Pu) par exécution du programme (P2) qui est la mise en oeuvre d'une transformation (T) combinatoire biunivoque, et tel que :

$$Pu = Du\ (T)\ Cu$$

où (Du) est un paramètre de diversification propre à chaque dispositif objet (CU3) et (Cu) une donnée propre à chaque dispositif objet (CU3),

- une mémoire (M4) où sont enregistrés une clé de base (Sb) et un programme (P3), et des circuits de traitement (T4) pour calculer un certificat (R1) par exécution du programme (P3) et tel que :

$$R1 = f3\ (K1, Ex)$$

avec $$K1 = Sb\ (T)\ Pu)$$

où (Ex) est une information externe.

14. Système selon la revendication (13), caractérisé en ce que la mémoire (M4) précitée contient également un programme (P1) exécuté par les circuits de traitement (T4) pour calculer le paramètre de diversification (Du) précité et qui prend en compte au moins une donnée (Eu) propre au dispositif objet (CU3).

15. Système selon la revendication 14, caractérisé en ce que le programme (P1) précité prend également en compte une clé intermédiaire (Sm) préenregistrée dans la mémoire (M4).

16. Système selon l'une des revendications 13 à 15, caractérisé en ce que la mémoire (M4) et les circuits de traitement (T4) sont intégrés dans un objet portatif (CM4) tel qu'une carte à mémoire.

17. Système selon l'une des revendications 13 à 15, caractérisé en ce que les mémoires (M4, M5) et les circuits de traitement (T4, T5) sont intégrés dans un boîtier à circuits intégrés.

18. Système selon la revendication 17, caractérisé en ce que le boîtier précité est logé dans un objet portatif tel qu'une à mémoire.

19. Système selon l'une des revendications 13 à 15, caractérisé en ce que la mémoire (M3) du dispositif objet (CU3) accouplée audit système contient un programme (P4) exécuté par les circuits de traitement (T3) pour calculer un certificat (R2) tel que :

$$R2 = f4\ (Ex,\ K2)$$

avec $$K2 = Sd\ (T)\ Cu$$

où (Ex) est l'information externe précitée, ce certificat (R2) devant être identique au certificat (R1) précité calculé par ledit système.

20. Système selon l'une des revendications 13 à 19, caractérisé en ce que le dispositif objet (CU3) est un objet portatif tel qu'une carte à mémoire.

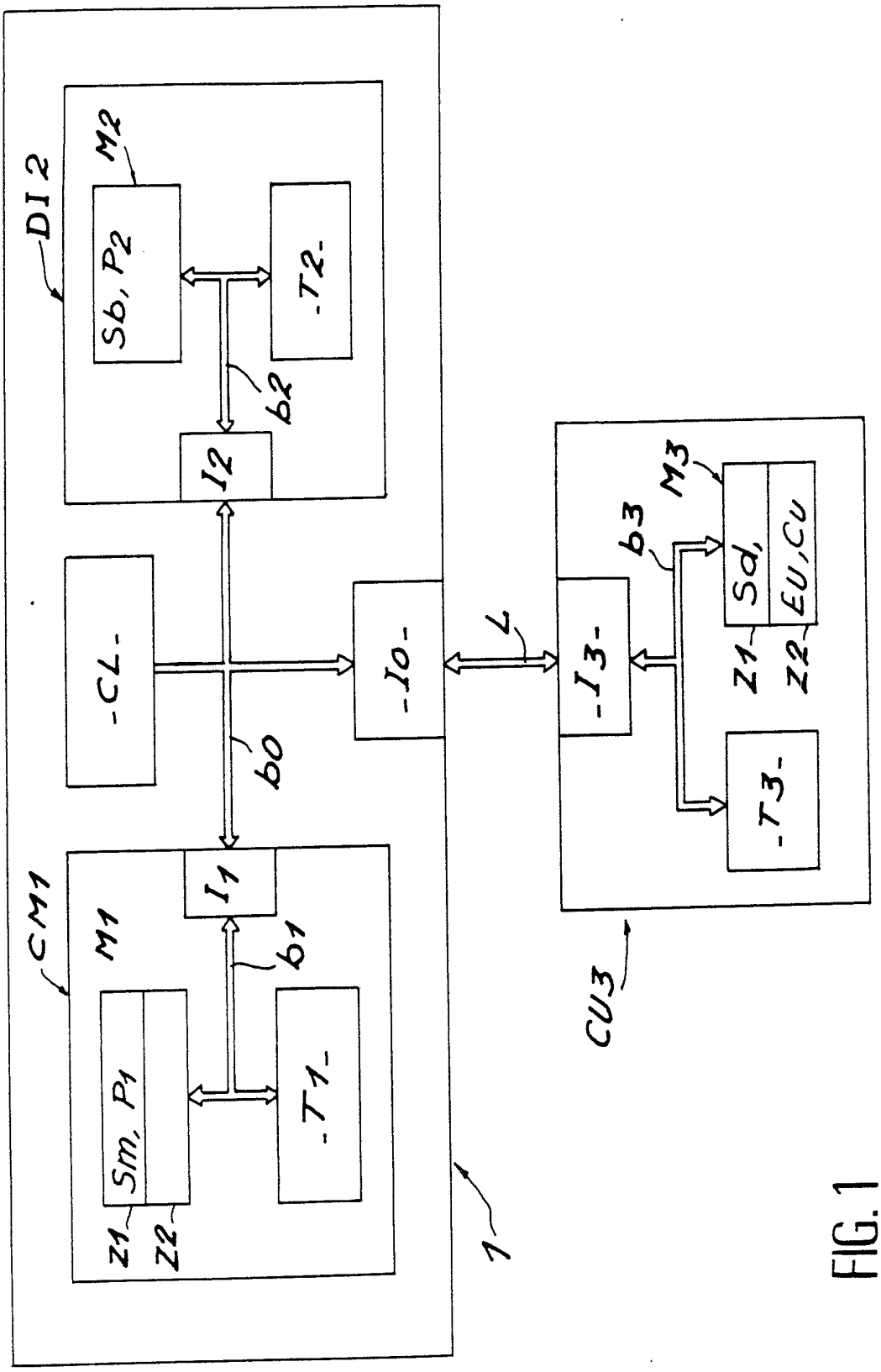

DI 2
M2
Sb, P2
-T2-
b2
I2
-CL-
b0
-IO-
L
-I3-
b3
M3
Sd,
Eu, Cu
Z1
Z2
-T3-
CU3
CM1
M1
I1
b1
Sm, P1
-T1-
Z1
Z2
1

FIG. 1

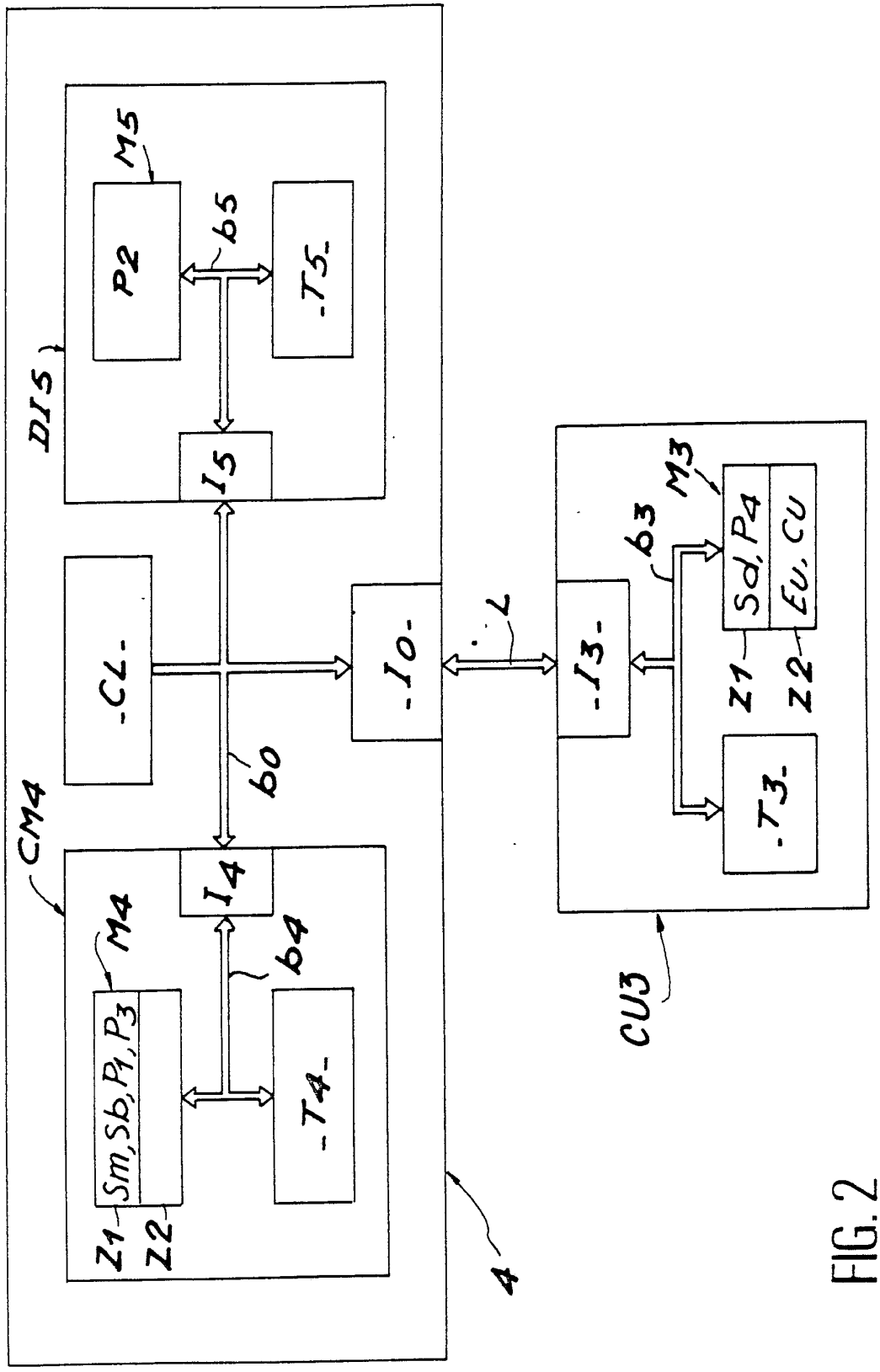

DIS
M5
P2
65
-T5-
I5
-CL-
-I0-
L
-I3-
63
M3
Sd, P4
Eu, Cu
Z1
Z2
-T3-
CU3
60
CM4
I4
M4
64
Sm, Sb, P1, P3
-T4-
Z1
Z2
4

FIG. 2

INTERNATIONAL SEARCH REPORT

International Application No PCT/FR87/00273

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) [6]

According to International Patent Classification (IPC) or to both National Classification and IPC

IPC[4]: G07F 7/10

II. FIELDS SEARCHED

Minimum Documentation Searched [7]

Classification System	Classification Symbols
IPC[4]	G07F, G06F, H04L

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched [8]

III. DOCUMENTS CONSIDERED TO BE RELEVANT [9]

Category *	Citation of Document, [11] with indication, where appropriate, of the relevant passages [12]	Relevant to Claim No. [13]
A	EP, A, 0055986 (TRANSAC-ALCATEL), 14 July 1982; see abstract; figure 1; page 2, lines 6-27, page 4, line 15-page 8, line 33; page 11, lines 1-33; claims 1-7 ---	1-20
A	EP, A, 0064779 (SVENSKA-PHILIPSFÖRETAGEN AB), 17 November 1982; see abstract; figures 1,3; page 5, line 4-page 8, line 5; page 9, line 25-page 10, line 30; page 13, line 6-page 14, line 6; claims 1-5 ---	1-20
A	EP, A, 0168667 (ATALLA-CORP.), 22 January 1986, see abstract; figure 1; page 2, lines 2-21; page 7, line 12-page 8, line 20; page 11, lines 1-19; claims 1-7 ---	1,3-12, 16-20
A	IBM Technical Disclosure Bulletin, Vol. 24, No. 12, May 1982 (New York, US), R.E. Lennon et al. : "Personal verification and message authentication using personal keys", pages 6504-6509, see the whole document ---	1,4,5,7, 10-20

../.

* Special categories of cited documents: [10]

"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

"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

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
12 October 1987 (12.10.87)	28 October 1987 (28.10.87)
International Searching Authority	**Signature of Authorized Officer**
European Patent Office	

III. DOCUMENTS CONSIDERED TO BE RELEVANT (CONTINUED FROM THE SECOND SHEET)

Category *	Citation of Document, with indication, where appropriate, of the relevant passages	Relevant to Claim No
A	EP, A, 0138386 (K.K. TOSHIBA), 24 April 1985, see abstract; figures 3-5,8,9B; page 1, lines 16-21; page 2, line 7-page 3, line 26; page 6, line 11-page 7, line 10; page 10, line 6-page 11, line 4; claims 1,2	1,4,7,10-13,16-18
A	EP, A, 0117907 (GABE GELDAUSGABEAUTOMATEN-SERVICE), 12 September 1984, see abstract; page 3, line 27-page 6, line 27; claim 1	1,7,13

ANNEX TO THE INTERNATIONAL SEARCH REPORT ON

INTERNATIONAL APPLICATION NO. PCT/FR 87/00273 (SA 17929)

This Annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report. The members are as contained in the European Patent Office EDP file on 20/10/87

The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP-A- 0055986	14/07/82	WO-A-	8202446	22/07/82
		FR-A-	2497617	09/07/82
		CA-A-	1169564	19/06/84
		US-A-	4498000	05/02/85
EP-A- 0064779	17/11/82	SE-A-	8102268	09/10/82
		SE-B-	426128	06/12/82
		CA-A-	1191916	13/08/85
EP-A- 0168667	22/01/86	JP-A-	61088363	06/05/86
EP-A- 0138386	24/04/85	JP-A-	60062252	10/04/85
EP-A- 0117907	12/09/84	None		

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale N° PCT/FR 87/00273

I. **CLASSEMENT DE L'INVENTION** (si plusieurs symboles de classification sont applicables, les indiquer tous) [7]

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

CIB[4]: G 07 F 7/10

II. **DOMAINES SUR LESQUELS LA RECHERCHE A PORTÉ**

Documentation minimale consultée [8]

Système de classification	Symboles de classification
CIB[4]	G 07 F G 06 F H 04 L

Documentation consultée autre que la documentation minimale dans la mesure où de tels documents font partie des domaines sur lesquels la recherche a porté [9]

III. **DOCUMENTS CONSIDÉRÉS COMME PERTINENTS** [10]

Catégorie *	Identification des documents cités,[11] avec indication, si nécessaire, des passages pertinents [12]	N° des revendications visées [13]
A	EP, A, 0055986 (TRANSAC-ALCATEL) 14 juillet 1982 voir résumé; figure 1; page 2, lignes 6-27, page 4, ligne 15 - page 8, ligne 33; page 11, lignes 1-33; revendications 1-7 --	1-20
A	EP, A, 0064779 (SVENSKA-PHILIPSFÖRETAGEN AB) 17 novembre 1982 voir résumé; figures 1,3; page 5, ligne 4 - page 8, ligne 5; page 9, ligne 25 - page 10, ligne 30; page 13, ligne 6 - page 14, ligne 6; revendications 1-5 --	1-20
A	EP, A, 0168667 (ATALLA-CORP.) 22 janvier 1986 voir résumé; figure 1; page 2, lignes 2-21; page 7, ligne 12 - page 8, ligne 20; page 11, lignes 1-19; revendications 1-7 -- ./.	1,3-12, 16-20

* Catégories spéciales de documents cités: [11]

« 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 postérieurement à la date de dépôt international ou à la date de priorité et n'appartenant 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'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive

« Y » document particulièrement pertinent; l'invention 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

IV. **CERTIFICATION**

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
12 octobre 1987	23 OCT 1987
Administration chargée de la recherche internationale	**Signature du fonctionnaire autorisé**
OFFICE EUROPEEN DES BREVETS	M. VAN MOL

III. DOCUMENTS CONSIDÉRÉS COMME PERTINENTS (SUITE DES RENSEIGNEMENTS INDIQUÉS SUR LA DEUXIÈME FEUILLE)

Catégorie *	Identification des documents cités, avec indication, si nécessaire, des passages pertinents	N° des revendications visées
A	IBM Technical Disclosure Bulletin, volume 24, no. 12, mai 1982 (New York, US) R.E. Lennon et al.: "Personal verification and message authentication using personal keys", pages 6504-6509 voir le document en entier	1,4,5,7,10-20
A	EP, A, 0138386 (K.K. TOSHIBA) 24 avril 1985 voir résumé; figures 3-5,8,9B; page 1, lignes 16-21; page 2, ligne 7 - page 3, ligne 26; page 6, ligne 11 - page 7, ligne 10; page 10, ligne 6 - page 11, ligne 4; revendications 1,2	1,4,7,10-13,16-18
A	EP, A, 0117907 (GABE GELDAUSGABEAUTOMATEN-SERVICE) 12 septembre 1984 voir résumé; page 3, ligne 27 - page 6, ligne 27; revendication 1	1,7,13

ANNEXE AU RAPPORT DE RECHERCHE INTERNATIONALE RELATIF

A LA DEMANDE INTERNATIONALE NO. PCT/FR 87/00273 (SA 17929)

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche international visé ci-dessus. Lesdits membres sont ceux contenus au fichier informatique de l'Office européen des brevets à la date du 20/10/87

Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets.

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevets		Date de publication
EP-A- 0055986	14/07/82	WO-A-	8202446	22/07/82
		FR-A-	2497617	09/07/82
		CA-A-	1169564	19/06/84
		US-A-	4498000	05/02/85
EP-A- 0064779	17/11/82	SE-A-	8102268	09/10/82
		SE-B-	426128	06/12/82
		CA-A-	1191916	13/08/85
EP-A- 0168667	22/01/86	JP-A-	61088363	06/05/86
EP-A- 0138386	24/04/85	JP-A-	60062252	10/04/85
EP-A- 0117907	12/09/84	Aucun		