

(19)



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11)

EP 0 833 281 A1

(12)

DEMANDE DE BREVET EUROPEEN

(43) Date de publication:
01.04.1998 Bulletin 1998/14

(51) Int Cl. 6: **G07C 9/00**

(21) Numéro de dépôt: **97401993.7**

(22) Date de dépôt: **27.08.1997**

(84) Etats contractants désignés:
**AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC
NL PT SE**

(30) Priorité: **28.08.1996 FR 9610516**

(71) Demandeur: **SAGEM SA
75116 Paris (FR)**

(72) Inventeur: **Zibell, Laurent
75015 Paris (FR)**

(74) Mandataire: **Bloch, Gérard
2, square de l'Avenue du Bois
75116 Paris (FR)**

(54) **Equipement de contrôle d'accès et badge d'accès pour cet équipement**

(57) Le badge (2) comporte une mémoire (8) pour le stockage d'une caractéristique physique particulière du porteur et des moyens radio (4) reliés à la mémoire (8). L'équipement comporte des moyens radio (11, 111) et pour lire dans la mémoire (8) du badge, des moyens

(15, 16) d'identification de la caractéristique physique particulière considérée du porteur du badge, un comparateur (17) relié en entrée aux moyens radio (11, 111) et aux moyens d'identification (15, 16) et, en sortie, à des moyens (20) de verrouillage de l'accès.

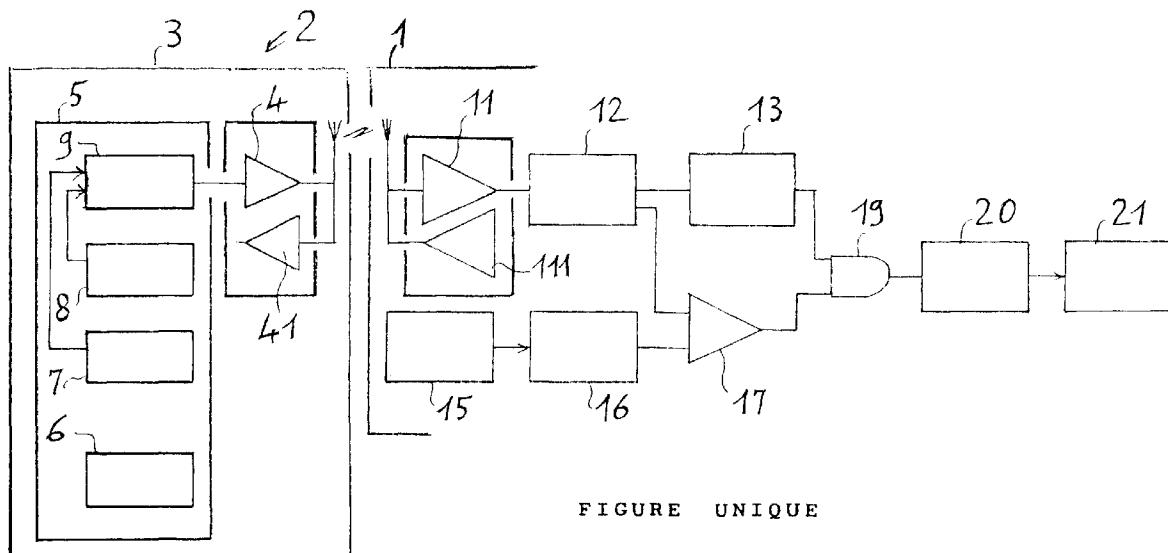


FIGURE UNIQUE

EP 0 833 281 A1

Description

Le contrôle d'accès à une zone protégée est de façon classique effectué par des équipements comportant un lecteur de badge, qui commande le déverrouillage de la porte d'accès que le lecteur contrôle. Le badge est une clé électronique contenant des informations d'autorisation d'accès, qui permet en particulier d'identifier son porteur afin de lui permettre l'accès à certaines zones et à le lui refuser pour d'autres, en fonction des informations mémorisées dans le lecteur, ou dans une base de données centrale. C'est donc le badge qui est identifié et c'est sa possession qui permet d'obtenir l'autorisation d'accès.

Afin de se prémunir contre le vol d'un badge, et vérifier que son titulaire et son porteur ne font qu'un, il est souvent prévu un clavier de saisie d'un mot de code, ou Numéro d'Identification Personnel (PIN, selon la terminologie anglaise) que le porteur doit fournir à l'équipement, pour s'identifier.

Il existe aussi des équipements dans lesquels l'identification du porteur de badge est effectuée par reconnaissance de ses empreintes digitales.

Dans tous les systèmes indiqués ci-dessus, le porteur doit effectuer deux saisies : il doit manuellement saisir son badge pour l'introduire dans le lecteur et il doit effectuer la saisie électronique du mot de code ou de ses empreintes. Le confort d'utilisation, ou la convivialité, d'un tel système à double opération laisse à désirer car le porteur du badge ne peut alors si besoin est, pousser simultanément la porte contrôlée. En outre, le temps nécessaire aux manipulations ci-dessus limite le débit de passage.

Pour améliorer la convivialité, il est connu de prévoir un passage sans contact au moyen d'un badge comportant un émetteur radio associé à une carte à puce contenant des informations d'autorisation d'accès et interrogée à distance par le lecteur, ce qui libère la main qui était nécessaire à la présentation du badge. Toutefois, la carte à puce ne comporte en général pas d'informations d'identification (PIN) du porteur. Mais si elle en contient, le temps de saisie de celui-ci obère, comme indiqué ci-dessus, la cadence de passage et encore la convivialité, ce qui incite l'exploitant à désactiver cette sécurité supplémentaire que constitue le mot de code PIN.

En outre, les transmissions radio entre le badge et le lecteur présentent l'inconvénient de risquer d'être captées par un tiers, qui est ainsi en mesure de reproduire, dans un badge en sa possession, les informations transmises, c'est-à-dire les autorisations d'accès mais aussi, bien souvent, le mot de code confidentiel PIN. La double sécurité que constituent le lecteur de badge et le clavier de saisie du mot de code PIN est alors prise en défaut.

L'invention vise à proposer un équipement de contrôle d'accès qui soit à la fois convivial et sûr.

A cet effet, l'invention concerne tout d'abord un

équipement de contrôle de l'accès à une zone protégée d'un porteur d'un badge, le badge comportant

- des moyens mémoires pour le stockage d'une caractéristique physique particulière du porteur,
- des moyens radio reliés aux moyens mémoires,

l'équipement comportant

- des moyens radio, agencés pour lire dans les moyens mémoires du badge,
- des moyens d'identification de la caractéristique physique particulière considérée du porteur du badge,
- des moyens de comparaison reliés en entrée aux moyens radio et aux moyens d'identification et, en sortie à des moyens de verrouillage de l'accès.

La demanderesse est allée à l'encontre de l'idée qui prévalait jusqu'alors, selon laquelle une transmission radio réduirait le niveau de sûreté du contrôle d'accès.

Une analyse plus approfondie du problème lui a fait découvrir en effet qu'il convenait de prendre en compte le fait que les caractéristiques physiques particulières du porteur diffèrent fondamentalement de données classiques. Ces dernières n'ont de valeur que par leur contenu, indépendamment de leur support, et peuvent donc être copiées sur un autre support semblable et être directement utilisées à des fins frauduleuses. Par contre, et même si les informations définies par les caractéristiques physiques d'une personne peuvent être copiées une fois qu'elles ont été transformées en données informatiques, numériques, il est impossible de les reconstituer sous leur forme analogique d'origine puisqu'elles font partie intégrante de la personne. Comme caractéristique de la personne, autres que les empreintes digitales, on peut songer à l'image de la rétine ou le code génétique.

De ce fait, il est alors apparu à la demanderesse que l'on pouvait parfaitement tolérer une réduction du niveau de sûreté au niveau de la lecture par radio du badge, puisque la saisie des caractéristiques physiques directement sur le porteur maintenait à elle-même un niveau élevé.

Le contrôle d'accès présente alors une bonne convivialité et permet un passage rapide, d'autant que la seule opération à effectuer par le porteur du badge est de se présenter aux moyens d'identification, sans devoir saisir de mot de code. En bref, le porteur du badge fournit en quelque sorte l'attribut de sa propre personne.

L'invention concerne aussi un badge de contrôle d'accès à une zone protégée, pour l'équipement de contrôle d'accès de l'invention, comportant des moyens radio commandés par des moyens de mémorisation agencés pour transmettre, à l'équipement de contrôle

d'accès, les données d'identification, représentatives d'une caractéristique physique spécifique à un titulaire du badge.

L'invention sera mieux comprise à l'aide de la description suivante de la forme de réalisation préférée de l'équipement de l'invention et du badge associé, en référence à la figure unique qui les représente schématiquement.

L'équipement de l'invention, portant la référence 1, comporte deux voies d'entrée de données de contrôle d'accès. D'une part, il est agencé pour coopérer avec un badge 2 de fourniture de données d'autorisation d'accès, indiquant un droit de passage à l'accès contrôlé. D'autre part, l'équipement 1 peut saisir ici les empreintes du porteur du badge 2. La constitution du badge 2 et celle de l'équipement 1 vont être précisées ci-dessous.

Le badge 2 comporte un boîtier 3 comportant un circuit émetteur radio 4, associé à un circuit radio récepteur de veille 41, agencé pour réveiller entre autres l'émetteur 4 lorsque le badge 2 entre dans la zone de couverture radio de l'équipement 1, indiquée plus loin.

Le boîtier 3 comporte ici un connecteur, non représenté, pour recevoir une carte à puce 5 portant un microprocesseur 6 de gestion des circuits de la carte 5, en particulier d'une mémoire 7 contenant les données d'autorisation d'accès. Dans cet exemple, il est prévu une mémoire 8 de données représentant l'image de l'empreinte d'un doigt déterminé du titulaire du badge 2 et un circuit d'embrouillage 9 alimenté en données par les mémoires 7 et 8 pour commander l'émetteur radio 4 à travers le connecteur ci-dessus. Le circuit de réveil 41 commande aussi le réveil des circuits 6 à 9, qui, en outre, sont réalisés dans une technologie à faible consommation, évitant une décharge accélérée de la pile, non représentée, alimentant localement les circuit 4 et 41 et la carte 5. Une réalisation intégrée d'un boîtier comportant tous les circuits ci-dessus ne serait pas à exclure.

L'équipement 1 comporte, sur la première voie d'entrée, un récepteur radio 11, associé à un émetteur 111 de réveil, déterminant la couverture radio indiquée ci-dessus, commandant le circuit 41 de réveil. Le récepteur 11 est relié en sortie à une mémoire de travail 12 de stockage temporaire des données lues dans les mémoires 7 et 8, comportant en entrée un circuit de désembrouillage complémentaire du circuit 9. Une première sortie de la mémoire 12 adresse, par les données d'autorisation d'accès lues dans la mémoire 7, une logique à mémoire base de données 13 fournissant en réponse un signal binaire d'autorisation d'accès, appliqué à une porte logique ET 19 à deux entrées commandant un électro-aimant 20 de verrouillage / déverrouillage d'un portillon 21 de contrôle d'accès à une zone protégée. La mémoire 13 équivaut à un comparateur comparant les données lues dans le badge 2 à des données locales homologues d'autorisation liées à l'équipement 1 et déterminant les attributs ou critères que doit pos-

séder le titulaire du badge 2 pour que celui-ci soit autorisé à franchir le portillon 21.

Sur une seconde voie, l'équipement 1 comporte un lecteur 15 de saisie d'images d'une partie du corps du porteur, ici l'image d'une zone de peau et plus précisément dans ce cas des empreintes digitales. Le lecteur 15, du genre scanner, est relié en sortie à un circuit 16 de traitement d'image qui extrait de l'image, saisie par le lecteur 15, les positions des points caractéristiques des empreintes, afin de réduire le volume mémoire nécessaire. Une image d'empreinte est ainsi caractérisée par les positions relatives, ou topologie, de ces points, représentant chacun par exemple les intersections entre sillons de l'empreinte.

Un comparateur 17 reçoit les données d'image déterminées par le circuit 16 et celles correspondantes de la mémoire 12, représentant les données de la mémoire 8 du badge 2, et, en cas de concordance, il fournit un signal d'identification du porteur du badge 2, appliqué à la deuxième entrée de la porte ET 19, indiquant qu'il est effectivement le titulaire du badge 2.

Lorsque la porte ET 19 détecte la présence simultanée des deux signaux, d'autorisation d'accès et d'identification, elle commande l'électro-aimant 20 pour déverrouiller le portillon 21.

Les autorisations d'accès peuvent indiquer un ou des attributs du titulaire du badge 2, par exemple la catégorie de personnel, ou le niveau hiérarchique, et la mémoire 13 autorise ou non l'accès en fonction de ce ou ces attributs. Un autre équipement semblable, contrôlant une autre voie d'accès à une autre zone, pourra avoir été initialisé (écriture de la mémoire 13) pour fournir une réponse différente, en fonction de critères justifiant l'accès à cette autre zone par certaines catégories de personnel ayant un attribut déterminé. La mémoire 13 équivaut ainsi à une logique à tables de décision d'accès adressées par des critères ou attributs.

Le fonctionnement de l'équipement 1 et du badge 2 va maintenant être expliqué plus en détails.

Lorsque le porteur du badge 2 s'approche de l'équipement 1 et pénètre dans sa zone de couverture radio, l'émetteur 111 réveille, par le récepteur 41, les circuits du badge 2 qui avaient été mis à l'état repos, à consommation réduite ou même interrompu par le circuit 41, alors non commandé. Le microprocesseur 20, réveillé, commande alors l'émission radio du contenu des mémoires 7 et 8, sous forme embrouillée (9).

La mémoire 12 mémorise ces données après les avoir débrouillées et celles-ci sont traitées comme cela a déjà été expliqué. Il aurait pu être prévu que le désembrouillage soit effectué au niveau des circuits 13 et 17 les exploitant.

Dans le même temps, le porteur du badge 2 doit apposer le doigt concerné sur le scanner 15 pour alimenter le circuit de traitement 16. La constellation des positions des points caractéristiques, qui a été de même préalablement saisie dans une étape de mise en service du badge 2 par chargement de sa mémoire 8 en parti-

culier, est alors comparée (17) à celle définie par les données de référence lues dans la mémoire 8. A titre d'exemple, on peut indiquer que cette comparaison peut s'effectuer par un traitement du signal équivalent à une translation et une rotation jusqu'à superposer parfaitement les positions (ou un grand pourcentage de celles-ci dans une zone de l'image). On peut encore songer à une détermination du niveau de corrélation entre images par comparaisons d'attributs de celles-ci, par exemple par détermination d'un spectre de distances entre points caractéristiques de l'image et par comparaison à un spectre homologue de référence (8).

Dans d'autres exemples, ce peut être l'image de la rétine du porteur de badge qui est saisie.

De même, les données d'autorisation pourraient encore se présenter sous forme directement explicite, et non plus sous forme d'attributs à interpréter par le lecteur, c'est-à-dire sous la forme d'une liste de zones, ou de portillons, individualisées dont l'accès est autorisé au titulaire du badge 2. Dans ce cas, le badge 2 ne ferait que transmettre cette autorisation à la porte 19, le circuit 13 étant alors quasi-transparent, c'est-à-dire que les données d'autorisation du badge 2 seraient validées, c'est-à-dire commanderaient la porte 19, par leur seul contenu,. A titre de protection, cependant, cette validation peut requérir que les données d'autorisation lues dans le badge présentent un format de clé électronique prédéterminé, dont le secret est ici protégé par l'embrouillage. Le circuit 13 ne contrôlerait alors que la concordance entre l'identité de l'équipement 2, stockée dans celui-ci, et l'une des identités d'une liste d'équipements semblables, à accès autorisé, liste présente dans les données d'autorisation lues dans le badge 2 et nécessaire dans le cas où les portillons ne peuvent être banalisés, du fait de l'existence de plusieurs zones protégées accessibles à des groupes de personnes au moins partiellement différents.

Hormis les moyens d'interface 11, 111 et 15, on comprendra que le reste des circuits de l'équipement 1 peut être déporté, par exemple dans un ordinateur en site central, commun à une pluralité de tels équipements 1.

Revendications

1. Equipement de contrôle de l'accès à une zone protégée d'un porteur d'un badge (2), le badge (2) comportant
 - des moyens mémoires (8) pour le stockage d'une caractéristique physique particulière du porteur,
 - des moyens radio (4) reliés aux moyens mémoires (8), l'équipement comportant
 - des moyens radio (11, 111), agencés pour lire

- dans les moyens mémoires (8) du badge,
- des moyens (15, 16) d'identification de la caractéristique physique particulière considérée du porteur du badge,
 - des moyens de comparaison (17) reliés en entrée aux moyens radio (11, 111) et aux moyens d'identification (15, 16) et, en sortie, à
 - des moyens (20) de verrouillage de l'accès.
2. Equipement selon la revendication 1, dans lequel, le badge (2) comportant des moyens (7) de mémorisation de données d'autorisation d'accès, il est prévu des moyens (12, 13) de validation des données d'autorisation du badge et reliés à l'entrée desdits moyens de verrouillage (20).
 - 20 3. Equipement selon la revendication 2, dans lequel, le badge (2) étant agencé pour transmettre les données d'autorisation sous forme embrouillée, les moyens de validation (12) sont agencés pour débrouiller celles-ci.
 - 25 4. Equipement selon la revendication 3, dans lequel les moyens de validation (13) sont agencés pour valider les données d'autorisation à partir de leur seul contenu.
 - 30 5. Equipement selon l'une des revendications 2 à 4, dans lequel les moyens de validation (13) comportent des moyens comparateurs agencés pour comparer les données d'autorisation lues à des données homologues stockées dans une base de données de l'équipement.
 - 35 6. Equipement selon l'une des revendications 1 à 5, dans lequel les moyens d'identification (15, 16) sont agencés pour saisir l'image de la rétine du porteur de badge.
 - 40 7. Equipement selon l'une des revendications 1 à 5, dans lequel les moyens d'identification (15, 16) sont agencés pour saisir l'image d'une empreinte de la peau du porteur.
 - 45 8. Equipement selon la revendication 7, dans lequel les moyens d'identification (15, 16) sont agencés pour saisir l'image d'une empreinte digitale.
 - 50 9. Badge (2) de contrôle d'accès à une zone protégée pour l'équipement de l'une des revendications là 8, comportant des moyens radio (4) commandés par des moyens de mémorisation (8) agencés pour transmettre, à un équipement de contrôle d'accès, des données d'identification, représentatives d'une caractéristique physique spécifique à un titulaire du

badge (2).

5

10

15

20

25

30

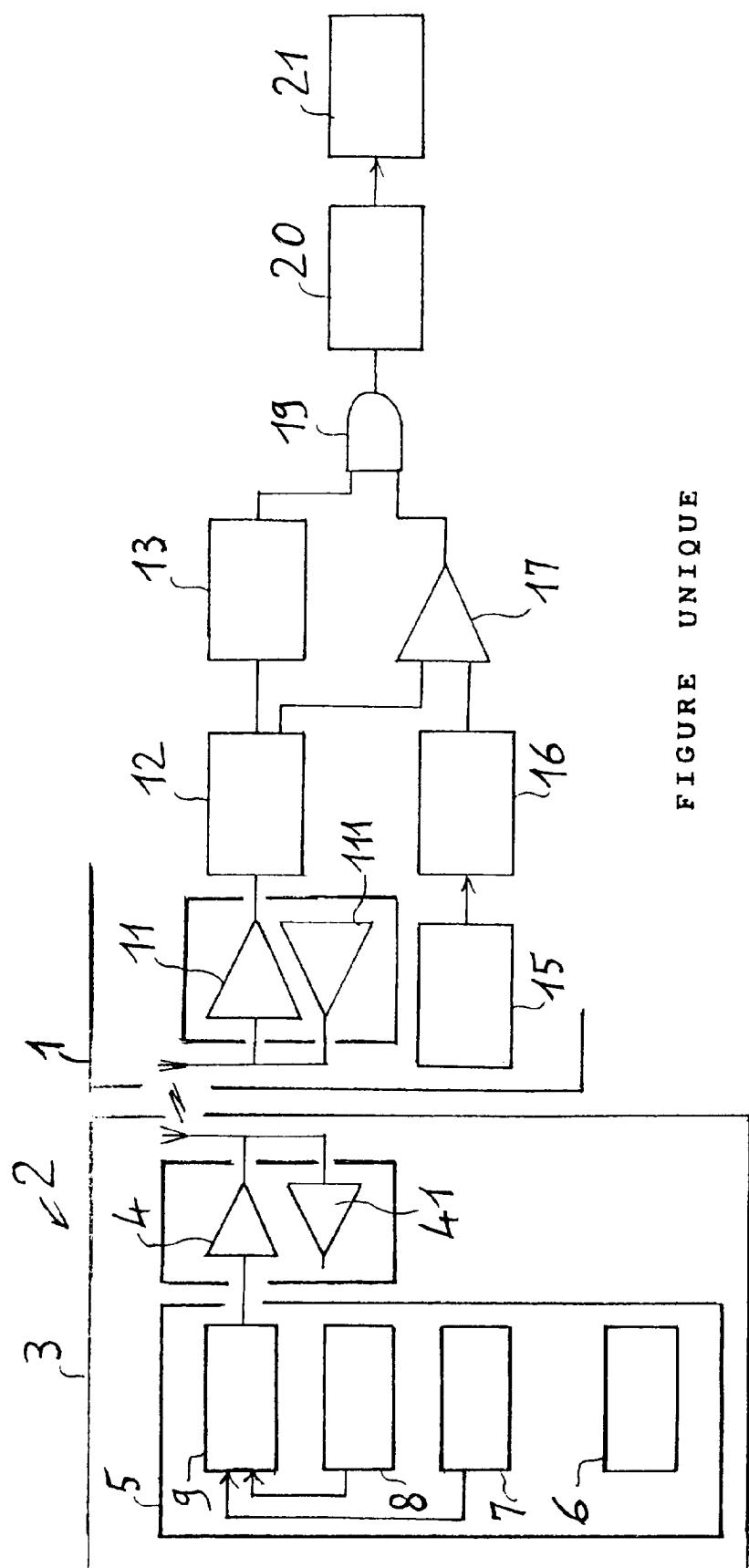
35

40

45

50

55





Office européen
des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 97 40 1993

DOCUMENTS CONSIDERES COMME PERTINENTS			
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Révendication concernée	CLASSEMENT DE LA DEMANDE (Int.Cl.6)
X	GB 2 181 582 A (BLACKWELL VICTOR CAMPBELL) 23 avril 1987 * abrégé; revendications; figures * * page 1, ligne 66 - page 2, ligne 28 * * page 2, ligne 89 - page 3, ligne 99 * ---	1,2,7-9	G07C9/00
X	WO 96 06409 A (GEEFIELD PTY LTD :CHAPMAN BRYAN P (AU)) 29 février 1996 * abrégé; revendications; figures * * page 3, ligne 18 - page 6, ligne 26 * * page 13, ligne 20 - page 15, ligne 31 * * page 17, ligne 5 - page 18, ligne 31 *	1-5,9	
Y	US 4 993 068 A (PIOSENKA GERALD V ET AL) 12 février 1991 * abrégé; revendications; figures * * colonne 3, ligne 28 - colonne 6, ligne 54 *	1-9	
Y	FR 2 615 984 A (TOKYO SHIBAURA ELECTRIC CO) 2 décembre 1988 * abrégé; revendications; figures * * page 10, ligne 9 - page 11, ligne 9 *	1-9	DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6)
A	WO 89 12287 A (TRIPEAU JEAN PIERRE) 14 décembre 1989 * abrégé; revendications; figures *	1,2,4, 7-9	G07C
A	EP 0 159 539 A (SIEMENS AG) 30 octobre 1985 * abrégé; revendications; figures *	1,7-9	
A	EP 0 102 109 A (PHILIPS NV) 7 mars 1984 * page 7, ligne 24 - page 9, ligne 3 * * page 14, ligne 10 - page 16, ligne 3: figures *	1,4,5,9 --- -/--	
Le présent rapport a été établi pour toutes les revendications			
Lieu de la recherche	Date d'achèvement de la recherche	Examinateur	
LA HAYE	8 décembre 1997	Meyl, D	
CATEGORIE DES DOCUMENTS CITES			
X : particulièrement pertinent à lui seul	T : théorie ou principe à la base de l'invention		
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie	E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date		
A : arrête-plan technologique	D : cité dans la demande		
O : divulgation non-écrite	L : cité pour d'autres raisons		
P : document intercalaire	S : membre de la même famille - document correspondant		



Office européen
des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numero de la demande
EP 97 40 1993

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.6)
A	FR 2 604 808 A (BAZIN GERARD) 8 avril 1988 * page 2, ligne 15 - page 5, ligne 9; figures *	1,2,9	
DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6)			
<p>Le présent rapport a été établi pour toutes les revendications</p>			
Lieu de la recherche	Date d'achèvement de la recherche	Examinateur	
LA HAYE	8 décembre 1997	Meyl, D	
CATEGORIE DES DOCUMENTS CITES			
X : particulièrement pertinent à lui seul	T : théorie ou principe à la base de l'invention		
Y : particulièrement pertinent en comparaison avec un autre document de la même catégorie	E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date		
A : arrrière-plan technologique	D : cité dans la demande		
O : divulgation non-écrite	L : cité pour d'autres raisons		
P : document intercalaire	& : membre de la même famille, document correspondant		