

(19)



Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

**EP 0 986 804 B1**

(12)

**FASCICULE DE BREVET EUROPEEN**

(45) Date de publication et mention  
de la délivrance du brevet:

**13.03.2002 Bulletin 2002/11**

(21) Numéro de dépôt: **98929501.9**

(22) Date de dépôt: **05.06.1998**

(51) Int Cl.7: **G09F 3/02, B65D 55/06**

(86) Numéro de dépôt international:  
**PCT/FR98/01150**

(87) Numéro de publication internationale:  
**WO 98/55984 (10.12.1998 Gazette 1998/49)**

(54) **COMPLEXE ET DISPOSITIF POUR GARANTIR L'INVOLABILITE ET L'AUTHENTICITE D'UN DOCUMENT OU D'UNE MARCHANDISE**

KOMPLEX UND VORRICHTUNG ZUR SICHERUNG DER ORIGINALITÄT VON DOKUMENTEN  
ODER GÜTERN

COMPLEX AND DEVICE FOR GUARANTEEING THE TAMPER-PROTECTION AND  
AUTHENTICITY OF A DOCUMENT OR GOODS

(84) Etats contractants désignés:  
**CH DE ES FR GB GR IT LI PT**

(30) Priorité: **06.06.1997 FR 9707051**

(43) Date de publication de la demande:  
**22.03.2000 Bulletin 2000/12**

(73) Titulaire: **Sequoias**  
**94220 Charenton (FR)**

(72) Inventeur: **TRAPLETTI, Claude**  
**F-94700 Maisons-Alfort (FR)**

(74) Mandataire: **Leszczynski, André**  
**NONY & ASSOCIES**  
**3, rue de Penthièvre**  
**75008 Paris (FR)**

(56) Documents cités:  
**EP-A- 0 656 614** **FR-A- 2 719 687**  
**US-A- 5 267 756** **US-A- 5 346 259**

**EP 0 986 804 B1**

Il est rappelé que: Dans un délai de neuf mois à compter de la date de publication de la mention de la délivrance du brevet européen, toute personne peut faire opposition au brevet européen délivré, auprès de l'Office européen des brevets. L'opposition doit être formée par écrit et motivée. Elle n'est réputée formée qu'après paiement de la taxe d'opposition. (Art. 99(1) Convention sur le brevet européen).

## Description

**[0001]** La présente invention concerne un complexe et un dispositif pour garantir l'inviolabilité et l'authenticité d'un document ou d'une marchandise, en vue d'éviter leur contrefaçon.

**[0002]** On connaît déjà des dispositifs destinés à garantir l'authenticité d'un document ou d'un produit, comme, par exemple, celui décrit par US-A-5 267 756. Ces dispositifs utilisent des techniques relativement complexes, souvent combinées entre elles.

**[0003]** Cependant, ces dispositifs connus ne donnent pas entière satisfaction, notamment du fait qu'ils sont souvent copiés, qu'ils ne permettent pas de contrôler l'authenticité d'un produit aux différentes étapes de sa vie, ni de détecter une copie frauduleuse d'un produit authentique existant.

**[0004]** La présente invention vise à éliminer ces inconvénients en proposant un dispositif qui permet en outre de garantir l'inviolabilité d'un produit.

**[0005]** L'invention permet donc d'exercer l'ensemble des contrôles réalisables au cours de la vie d'un produit, c'est-à-dire avant sa vente, lors de sa vente ou de sa mise en service, durant sa vie chez un consommateur et jusqu'à la fin de sa vie.

**[0006]** L'invention s'applique d'une manière générale à tout objet, ce dernier pouvant être par exemple un document papier, une enveloppe, une marchandise ou son emballage.

**[0007]** La présente invention a tout d'abord pour objet un complexe destiné à garantir l'inviolabilité et l'authenticité d'un objet comprenant :

- un support de base solidarisé de manière définitive à l'objet et sur lequel sont imprimés un code d'identification et au moins un code d'authentification,
- une feuille protectrice recouvrant partiellement le support de base pour protéger le code d'authentification et apte à être appliquée sur l'objet de manière à en assurer l'inviolabilité,
- des informations concernant l'objet lui-même portées sur la partie non recouverte du support de base.

**[0008]** Le support de base peut être constitué par l'emballage de l'objet ou même une partie de l'objet susceptible de recevoir une impression, ou encore par une étiquette collée fermement sur l'objet.

**[0009]** L'étiquette et la feuille protectrice peuvent être constituées en différents matériaux tels qu'un papier, une matière plastique, un tissu, du bois, du cuir etc...

**[0010]** Le code d'identification peut être imprimé par tout procédé connu d'impression sur le support de base. On peut utiliser à cet effet une encre fluorescente, invisible à l'oeil humain et nécessitant un dispositif de lecture particulier.

**[0011]** Le code d'authentification imprimé sur le support de base est de préférence masqué par une couche

opaque d'un matériau grattable, c'est-à-dire d'un matériau qui peut être éliminé par grattage pour révéler le code d'authentification, tel que celui que l'on utilise pour masquer des codes d'authentification sur des billets de loteries d'Etat.

**[0012]** Dans ce cas, la feuille protectrice peut être transparente, ce qui permet de montrer au consommateur qu'il disposera de moyens de contrôle de l'authenticité du produit et que le fabricant assurera un suivi du produit, ce qui est un gage de qualité de ce dernier.

**[0013]** En l'absence de couche opaque grattable sur le ou les codes d'authentification, la feuille protectrice sera obligatoirement opaque.

**[0014]** La feuille protectrice assure une double protection de l'objet du fait qu'elle rend inaccessible et éventuellement invisible le code d'authentification et qu'elle constitue un témoin d'inviolabilité pour l'objet protégé, garantissant ainsi que ce dernier n'a été ni ouvert ni utilisé.

**[0015]** Les informations concernant l'objet lui-même sont par exemple des informations portées sur le support de base par le fabricant de l'objet au moment de sa fabrication. Il peut s'agir de la date et du lieu de production, de l'équipe de production, du type de produit, etc...

**[0016]** Le complexe selon l'invention est destiné à être mis en oeuvre en combinaison avec des fichiers tenus par le fabricant des complexes et par l'utilisateur desdits complexes, qui les applique sur des objets à protéger.

**[0017]** La présente invention a donc également pour objet un dispositif destiné à garantir l'inviolabilité et l'authenticité d'un objet, caractérisé par le fait qu'il comprend des complexes tels que décrits ci-dessus et au moins un fichier de liens contenant le code d'identification de chaque complexe en relation avec son code d'authentification, ainsi qu'un fichier d'authentification contenant, en relation avec le code d'authentification de chaque complexe, les informations concernant l'objet protégé portées sur la partie non recouverte du support de base dudit complexe.

**[0018]** Selon l'invention, seul le fabricant des complexes, qui est en général un imprimeur travaillant en univers sécurisé, c'est-à-dire respectant différentes procédures garantissant la confidentialité des informations, connaît le fichier de liens qui relie les codes d'identification et les codes d'authentification portés par les complexes.

**[0019]** Etant donné qu'à ce stade, on ne connaît pas la destination des complexes, toute copie frauduleuse du fichier de liens serait infructueuse car il est impossible de savoir sur quels objets les complexes vont être appliqués.

**[0020]** La mise en oeuvre des complexes s'effectue de la manière suivante :

- 1°) Le fabricant des complexes imprime sur chaque support de base un code d'identification et au moins un code d'authentification et met à jour son fichier

de liens, mémorisant ainsi les n-uplets (code d'identification, codes d'authentification) qu'il crée sans connaître la destination des complexes.

2°) Le fabricant recouvre ensuite avec une feuille protectrice la partie du support de base portant le ou les codes d'authentification, après avoir éventuellement masqué ces codes d'authentification avec une couche opaque d'un matériau grattable. La feuille protectrice dépasse éventuellement du support de base de manière à pouvoir être collée sur l'ouverture d'un objet à protéger pour en assurer l'inviolabilité.

Cette feuille comporte également des découpes délimitant une ou plusieurs fenêtres qui donnent accès chacune à un code d'authentification du complexe. Chaque fenêtre ne peut être ouverte que d'une manière définitive, ce qui permet de décoder tout accès non autorisé à un code d'authentification.

[0021] Dans une variante, un code d'authentification peut être imprimé avec une encre magnétique, ce qui permet de lire ce code à travers la feuille et éventuellement la couche opaque qui le recouvre. On utilise à cet effet un lecteur magnétique.

3°) L'utilisateur des complexes, qui est en général un fabricant d'objets à protéger, reçoit du fabricant des complexes une copie du fichier de liens et un lot de complexes correspondant.

4°) L'utilisateur applique sur chaque objet qu'il souhaite protéger un complexe qu'il personnalise en imprimant sur ce dernier des informations concernant l'objet, comme par exemple un code produit, une date de fabrication, un numéro de lot etc...

5°) Simultanément, l'utilisateur met à jour un fichier central construit sur la base du fichier de liens, en y reportant toutes les informations concernant l'objet, en relation avec le code d'authentification.

6°) L'utilisateur scinde ensuite ce fichier central en deux fichiers distincts, à savoir un fichier d'authentification qui contient les codes d'authentification et les informations concernant les objets préalablement mises à jour et un fichier de gestion qui ne contient que les codes d'identification et des informations destinées à organiser la distribution des objets par des moyens logistiques traditionnels.

[0022] L'ensemble du dispositif permet de contrôler l'authenticité de l'objet à différents stades de sa vie.

[0023] Tout d'abord, chez un distributeur, un inspecteur assermenté par le fabricant récupère un code d'authentification porté par le complexe en ouvrant la fenêtre qui lui est destinée ou en lisant, à travers la feuille protectrice et à l'aide d'un lecteur magnétique, le code d'authentification qui lui est destiné, si ce dernier est imprimé avec une encre magnétique.

[0024] L'inspecteur envoie le code d'authentification récupéré au fabricant des objets, lequel consulte son

fichier d'authentification et indique à l'inspecteur d'une part, si l'objet appartient à l'ensemble des objets mis en circulation par le fabricant et d'autre part, les informations concernant l'objet contenues par le fichier, informations que l'inspecteur peut comparer à celles imprimées en clair sur le complexe.

[0025] Cet échange de données peut bien entendu être automatisé par des moyens télématiques.

[0026] En cas d'inexistence du code d'authentification dans le fichier d'authentification tenu par le fabricant ou de discordance entre les informations portées en clair sur le complexe et celles contenues dans le fichier, une contrefaçon est présumée et une procédure de contrôle peut être déclenchée.

[0027] Pour éviter que ce contrôle ne soit effectué par une personne non habilitée, la transmission du code d'authentification s'accompagne d'un mot de passe connu seulement de l'inspecteur. A défaut du mot de passe correct, le fabricant détecte une tentative frauduleuse et ne fournit pas la réponse attendue.

[0028] Lors de chaque contrôle, le fabricant enregistre dans le fichier d'authentification la trace du contrôle effectué, par exemple en mémorisant la date et la nature du contrôle.

[0029] Lors de la vente de l'objet, le distributeur procède de même en utilisant le code d'authentification qui lui est destiné et le mot de passe qui lui a été attribué.

[0030] Le fabricant vérifie à cette occasion que l'objet est bien enregistré dans son fichier d'authentification comme se trouvant en état d'être vendu. Si l'objet a déjà été vendu, une anomalie est détectée.

[0031] La trace du contrôle est également enregistrée dans le fichier d'authentification, avec d'autres informations relatives à la vente telles que sa date, son lieu et des informations portant sur le consommateur et permettant de réaliser ultérieurement des statistiques.

[0032] Dans le cas, d'un bien d'équipement ou plus généralement d'un produit garanti, une fois le contrôle effectué, le commerçant envoie au fabricant le numéro préimprimé d'un bon de garantie ou d'un bordereau de service après vente, émet ce bon ou ce bordereau, puis imprime sur ce dernier un nouveau code d'authentification qui est lui fourni en réponse par le fabricant pour lier le numéro du bon ou du bordereau à l'objet protégé. Le nouveau code d'authentification est simultanément enregistré dans le fichier d'authentification tenu par le fabricant.

[0033] Le consommateur ayant acheté l'objet peut également en vérifier l'authenticité. A cet effet, lors de l'ouverture de l'objet, il détruit définitivement la feuille protectrice qui témoignait de l'inviolabilité de l'objet et découvre le code d'authentification qui lui est destiné. Le consommateur peut également prendre connaissance de ce code avant d'ouvrir l'objet, en ouvrant une fenêtre dans la feuille opaque et en grattant la couche grattable qui masque son code d'authenticité. Connaissant ce code, le consommateur peut interroger le fabricant soit par téléphone, soit par des moyens télémati-

ques. Le fabricant peut ainsi vérifier que l'objet est bien enregistré comme ayant été vendu et renvoie au consommateur des informations générales sur l'objet, informations que le consommateur peut comparer à celles portées en clair sur le complexe associé à l'objet.

**[0034]** Plus tard, après avoir utilisé l'objet, le consommateur peut faire appel au service après-vente du fabricant. Le bon de garantie ou le bordereau de service après-vente fournit alors un code d'authentification qui permet d'effectuer les mêmes vérifications auprès du fabricant, ce dernier pouvant en outre mettre à jour son fichier d'authentification en y enregistrant la trace de l'intervention du service après-vente.

**[0035]** Dans un mode de réalisation particulier, le complexe comporte, dans la partie du support de base non recouverte par la feuille protectrice, une clé de contrôle générée par un algorithme sur la base d'une part du code d'authentification du complexe, d'autre part, d'une information spécifique à l'objet protégé, par exemple sa date et son heure de fabrication. Cette information spécifique doit apparaître de façon lisible sur le support de base.

**[0036]** Dans ce mode de réalisation, on utilise un code d'authentification imprimé avec une encre magnétique de manière à pouvoir le lire à travers la feuille protectrice à l'aide d'un lecteur magnétique.

**[0037]** Le lecteur magnétique est fourni à chaque intervenant du réseau de distribution, par exemple au commerçant qui vend l'objet.

**[0038]** Un microprocesseur exécutant le même algorithme que celui qui a servi à générer la clé de contrôle est intégré au lecteur magnétique. Ce microprocesseur est enfermé dans une capsule inviolable de manière à s'autodétruire en cas de tentative de lecture de l'algorithme.

**[0039]** Le commerçant peut ainsi vérifier l'authenticité de l'objet en faisant lire le code d'authentification par le lecteur magnétique et en saisissant les informations spécifiques à l'objet qu'il lit sur la partie visible du support de base. Le microprocesseur inclus dans le lecteur magnétique génère à nouveau une clé de contrôle à partir du code d'authentification lu et des informations spécifiques saisies.

**[0040]** Le commerçant n'a qu'à comparer la clé de contrôle ainsi générée avec celle imprimée en clair sur le support de base pour vérifier l'authenticité de l'objet.

**[0041]** Ce mode de réalisation permet, sans dégrader le complexe, de vérifier l'authenticité de la quasi-totalité d'un stock d'objets. Cette vérification ne garantit pas la même fiabilité que celle consistant à interroger le fichier d'authentification du fabricant mais elle peut la compléter. En effet, on peut limiter l'interrogation du fichier du fabricant à un échantillon relativement réduit du stock et vérifier le reste du stock grâce aux clés de contrôle.

**[0042]** Afin de pouvoir utiliser un même lecteur magnétique pour 5 effectuer un contrôle sur des objets provenant de fabricants différents, le microprocesseur peut être monté sur une carte à puce enfichable dans le lec-

teur. Chaque fabricant fournit alors sa propre carte à puce au commerçant.

**[0043]** Dans une variante, la clé de contrôle est masquée par une couche grattable de matériau opaque, et éventuellement protégée par une fenêtre de la feuille protectrice.

**[0044]** Dans une variante préférée de ce mode de réalisation, la clé de contrôle est générée par l'algorithme sur la base du code d'authentification du complexe et du code d'identification de l'objet protégé.

**[0045]** La clé de contrôle ainsi obtenue est imprimée dans la partie du support de base recouverte par la feuille protectrice, de préférence en étant noyée dans le code d'authentification.

**[0046]** Lors du contrôle, les codes d'authentification et d'identification sont relus et la clé de contrôle est régénérée puis comparée à celle imprimée sous la feuille protectrice et le microprocesseur fournit une réponse positive ou négative selon que la clé régénérée est identique à celle qui est noyée dans le code d'authentification.

**[0047]** Comme cela a déjà été précisé, le microprocesseur est de préférence intégré dans une carte à puce, également désignée carte à mémoire, enfichable dans un dispositif de lecture. Le microprocesseur comporte une mémoire qui contient l'algorithme de génération de la clé de contrôle ainsi que les positions de la clé de contrôle à lire sur le support de base entre les caractères constituant le code d'authentification.

**[0048]** Par exemple le code d'authentification peut se trouver aux positions 1, 3, 5, 6, 7, 9 d'une suite de 9 caractères dont les positions 2, 4, 8 correspondent à la clé de contrôle.

**[0049]** Cette variante permet de fournir une présomption d'authentification et de réaliser, dans un second temps, un contrôle complet du produit par consultation du fichier central, en regroupant plusieurs contrôles complets en une seule transaction à intervalles de temps réguliers, par exemple toutes les deux ou trois heures.

**[0050]** Cette variante peut notamment être utilisée dans des applications professionnelles dans les domaines de la pharmacie, des pièces détachées de véhicules automobiles ou de la distribution de tickets de loterie d'Etat, où l'établissement systématique de communications pour consultation du fichier central risque de poser des problèmes pratiques.

**[0051]** Le dispositif selon l'invention permet donc de lutter efficacement contre des contrefaçons d'objets commercialisés et de suivre l'évolution des objets protégés depuis leur fabrication jusqu'à leur utilisation par un consommateur.

**[0052]** Dans le but de mieux faire comprendre l'invention, on va en décrire maintenant un mode de réalisation donné à titre d'exemple non limitatif, en référence au dessin annexé dans lequel :

- la figure 1 représente un complexe destiné à être

- appliqué sur un flacon,
- la figure 2 représente le goulot du flacon recouvert par le complexe de la figure 1,
- les figures 3 à 8 sont des organigrammes retraçant les différentes étapes des opérations de contrôle d'authenticité.

**[0053]** Le complexe représenté sur la figure 1 comporte une étiquette 1 en tant que support de base et une feuille protectrice opaque 2.

**[0054]** L'étiquette est de forme rectangulaire, elle est réalisée en papier recouvert sur son verso d'une couche de colle forte.

**[0055]** La feuille opaque présente la forme d'un T. Elle est réalisée en PVC.

**[0056]** La feuille opaque 2 recouvre partiellement l'étiquette 1 dans la partie centrale de cette dernière.

**[0057]** Conformément à l'invention, l'étiquette comporte, dans sa partie non recouverte par la feuille opaque, un code d'identification 3 ainsi que des informations 4 concernant l'objet sur lequel le complexe doit être collé.

**[0058]** Dans sa partie centrale, l'étiquette comporte en outre trois codes d'identification 5,6,7 masqués chacun par une couche d'un matériau opaque grattable 8,9,10.

**[0059]** Ces trois codes d'identification et leur couche grattable sont recouverts par la partie de la feuille opaque 2 qui est collée sur l'étiquette.

**[0060]** Des fenêtres 11,12,13 sont découpées dans la feuille opaque en regard de chaque couche grattable 8,9,10.

**[0061]** Des découpes pleine chair 14 de la feuille opaque 2 permettent de révéler que cette dernière a été décollée de l'objet, le cas échéant.

**[0062]** Dans la partie de la feuille opaque recouvrant l'étiquette, ces découpes se trouvent en correspondance d'autres découpes pleine chair réalisées dans l'étiquette afin de révéler toute tentative de décollement de la feuille opaque et/ou de l'étiquette.

**[0063]** Des signes d'identification 15 sont en outre placés à cheval sur la feuille opaque 2 et sur l'étiquette 1. Ces signes d'identification se détruisent lorsque l'on sépare la feuille opaque de l'étiquette, par exemple lorsque l'on ouvre l'objet protégé.

**[0064]** D'autres signes d'authentification (non représentés) peuvent être prévus comme par exemple une taille douce, une impression iridescente ou des fils de sécurité.

**[0065]** Le complexe de la figure 1 est destiné à être collé sur un flacon, par exemple un flacon de parfum comme représenté à la figure 2.

**[0066]** Le flacon 16 de la figure 2 comporte un bouchon 17 qui coiffe son goulot. La grande face frontale 18 du flacon 16 est plane et se situe dans le même plan qu'un méplat 19 du bouchon 17. Le complexe est collé d'une part sur la grande face frontale 18 du flacon, qui reçoit l'étiquette 1 et la partie verticale du T de la feuille

opaque 2, tandis que le capuchon reçoit la partie horizontale du T collée sur sa surface latérale et collée sur elle-même à son extrémité.

**[0067]** On comprend que le complexe peut ainsi constituer un témoin d'inviolabilité du flacon car toute action exercée sur le capuchon entraînerait la destruction des différents signes d'authentification prévus sur la feuille opaque et sur l'étiquette, voire la destruction de ces dernières.

**[0068]** On va maintenant expliquer, en référence aux figures 3 à 8, la mise en oeuvre du complexe précédemment décrit.

**[0069]** La figure 3 est un organigramme des différentes étapes de la fabrication des complexes.

**[0070]** Lors d'une étape 30, on détermine le graphisme des complexes en dessinant d'une part les étiquettes, et d'autre part, les feuilles opaques.

**[0071]** Lors d'une étape 31, on imprime sur l'étiquette le code d'identification 3 et les codes d'authentification 5,6,7 préparés par des moyens informatiques lors d'une étape 32.

**[0072]** A l'étape 33, on couche un matériau opaque sur les codes d'authentification pour les masquer, puis on façonne l'étiquette et la feuille opaque et on les réunit à l'étape 34. Un contrôle de qualité est effectué à l'étape 35 pour éliminer les complexes présentant un défaut.

**[0073]** Parallèlement à la fabrication des complexes, les moyens informatiques génèrent un fichier de liens 36 qui établit la relation entre chaque code d'identification et les codes d'identification correspondants.

**[0074]** A l'étape 35 de contrôle de qualité, on informe les moyens informatiques de l'élimination des étiquettes défectueuses en vue de la suppression des enregistrements correspondants dans le fichier de liens 36.

**[0075]** Le fichier de liens 36 et le stock de complexes obtenus sont livrés à l'étape 37 à un utilisateur qui est ici un fabricant de flacons.

**[0076]** L'organigramme de la figure 4 indique les étapes mises en oeuvre par le fabricant pour personnaliser les complexes.

**[0077]** A partir des flacons 40 manufacturés par le fabricant et des complexes 1+2 reçus de l'imprimeur, le fabricant imprime sur les parties non recouvertes de l'étiquette 1 des informations 4 concernant les flacons qu'il désire protéger.

**[0078]** Ces informations de personnalisation des complexes sont simultanément mises à jour dans un fichier central 42 construit sur la base du fichier de liens 36 et dont chaque enregistrement comprend les informations de personnalisation 4.

**[0079]** Le fabricant scinde ensuite le fichier central 42 en un fichier d'authentification 43 et un fichier de gestion 44.

**[0080]** Le fichier d'authentification 43 contient, pour chaque flacon, les trois codes d'authentification du complexe correspondant et les informations de personnalisation 4, ainsi que des champs libres pour des informations ultérieures.

[0081] Le fichier de gestion 44 contient le code d'identification 3 ainsi que d'autres informations permettant l'organisation de la distribution commerciale des flacons.

[0082] Le fichier de gestion 44 est confié à des équipes logistiques 45 tandis que le fichier d'authentification 43 demeure entre les seules mains du fabricant.

[0083] En scindant le fichier central 42 en deux fichiers distincts, le fabricant perd toute possibilité d'établir un lien entre les informations concernant un flacon et le code d'identification porté par ce flacon.

[0084] Le contrôle de l'authenticité d'un flacon s'effectue suivant l'organigramme représenté à la figure 5.

[0085] Lors d'une étape 50, un inspecteur assermenté chargé de contrôler l'authenticité d'un flacon, arrache la fenêtre 15 de la feuille opaque 2 et gratte la couche opaque 10 pour découvrir le code d'authentification 7 qui lui est destiné, puis envoie ce code d'authentification 7 accompagné de son mot de passe 51 au fabricant.

[0086] Lors de l'étape 52, le fabricant interroge son fichier d'authentification 43 et retourne sa réponse 53, indiquant ainsi à l'inspecteur si le flacon est ou non authentique.

[0087] Simultanément, les informations concernant le flacon sont envoyées à l'inspecteur pour comparaison avec celles figurant sur l'étiquette 1.

[0088] A l'étape 54, l'inspecteur décide s'il est nécessaire de déclencher une procédure de contrôle en fonction de la réponse reçue du fabricant.

[0089] A l'étape 55, le fabricant enrichit son fichier d'authentification 43 en y enregistrant la trace du contrôle effectué, si ce dernier a été positif.

[0090] Sur la figure 6, on a représenté un organigramme du contrôle d'authenticité mis en oeuvre par un distributeur au moment de la vente du flacon.

[0091] A l'étape 60, le distributeur arrache la fenêtre 14, gratte la couche opaque 9 et découvre le code d'authentification 6 qu'il envoie au fabricant en même temps que son mot de passe personnel.

[0092] Cet envoi peut s'effectuer au travers d'un dispositif de connexion 61 relié au fabricant.

[0093] Ce dernier interroge son fichier d'authentification 43 et vérifie à l'étape 62 l'authenticité du flacon. La réponse 63 du fabricant est retournée au distributeur avec un nouveau code d'authentification que le distributeur saisit à l'étape 64.

[0094] Simultanément, le fabricant enrichit son fichier d'authentification à l'étape 65 en enregistrant le nom du point de vente et des informations générales sur le consommateur.

[0095] A l'étape 65, le distributeur émet un bon de garantie numéroté 66 sur lequel il imprime le nouveau code d'authentification reçu du fabricant.

[0096] La figure 7 illustre une opération de contrôle d'authenticité effectuée par un consommateur 70 ayant acheté le flacon.

[0097] Après avoir arraché la fenêtre 13 et découvert le code d'authentification 5 masqué par la couche grat-

table 8, le consommateur interroge le fabricant soit par téléphone, soit par des moyens télématiques.

[0098] En fonction du code d'authentification fourni au fabricant, ce dernier interroge son fichier d'authentification 43 et confirme au consommateur l'authenticité du flacon.

[0099] Ultérieurement, si le flacon s'avère défectueux, le consommateur peut faire jouer la garantie en mettant en oeuvre les étapes illustrées à la figure 8.

[0100] A l'étape 80, le consommateur envoie au fabricant le code d'authentification figurant sur son bon de garantie ainsi que son propre code d'authentification.

[0101] Le fabricant interroge le fichier d'authentification 43 à l'étape 81 et vérifie que le bon de garantie ainsi identifié est bien celui qui est lié au flacon en possession du consommateur.

[0102] La réponse du fabricant est adressée au consommateur à l'étape 82.

[0103] Cette opération de contrôle d'authenticité après la vente du produit peut aussi être exécutée par un service après-vente ou par le distributeur.

[0104] A l'étape 83, le fabricant enrichit, son fichier d'authentification en y enregistrant, par exemple, la date de mise en oeuvre de la garantie.

[0105] Il est bien entendu que le mode de réalisation qui vient d'être décrit ne présente aucun caractère limitatif et qu'il pourra recevoir toutes modifications désirables sans sortir pour cela du cadre de l'invention.

## Revendications

1. Complexe destiné à garantir l'inviolabilité et l'authenticité d'un objet comprenant :

- un support de base (1) solidarisé de manière définitive à l'objet (16) et sur lequel sont imprimés un code d'identification (3) et au moins un code d'authentification (5,6,7), **caractérisé par le fait qu'il comporte en outre:**
- une feuille protectrice (2), éventuellement opaque, recouvrant partiellement le support de base (1) pour protéger le code d'authentification (5,6,7) et apte à être appliquée sur l'objet (16) de manière à en assurer l'inviolabilité, et
- des informations (4) concernant l'objet (16) lui-même portées sur la partie non recouverte du support de base (1).

2. Complexe selon la revendication 1, **caractérisé par le fait que** le code d'authentification (5,6,7) imprimé sur le support de base masqué par une couche opaque d'un matériau grattable (8,9,10).

3. Complexe selon l'une quelconque des revendications 1 et 2, **caractérisé par le fait que** la feuille

protectrice (2) constitue un témoin d'inviolabilité pour l'objet (16) protégé, garantissant que ce dernier n'a été ni ouvert ni utilisé.

4. Complexe selon l'une quelconque des revendications 1 à 3, **caractérisé par le fait qu'il** comporte un code d'authentification imprimé avec une encre magnétique lisible à travers la feuille protectrice. 5
5. Complexe selon la revendication 4, **caractérisé par le fait qu'il** comporte, dans la partie de support de base (1) non recouverte par la feuille protectrice (2), une clé de contrôle générée par un algorithme sur la base d'une part, du code d'authentification (5,6,7) du complexe, d'autre part, d'une information spécifique à l'objet protégé (16) apparaissant de façon lisible sur le support de base (1). 10
6. Dispositif destiné à garantir l'inviolabilité et l'authenticité d'un objet, **caractérisé par le fait qu'il** comprend des complexes (1,2) selon l'une quelconque des revendications 1 à 5 et au moins un fichier de liens (36) contenant le ou les codes d'identification (3) de chaque complexe en relation avec son code d'authentification (5,6,7), ainsi qu'un fichier d'authentification (42) contenant, en relation avec le code d'authentification (5,6,7) de chaque complexe, les informations (4) concernant l'objet protégé (16) portées sur la partie non recouverte du support de base (1) dudit complexe. 15 20 25 30
7. Dispositif destiné à garantir l'inviolabilité et l'authenticité d'un objet, **caractérisé par le fait qu'il** comprend un complexe (1,2) selon la revendication 5, et un lecteur magnétique dans lequel est intégré un microprocesseur exécutant le même algorithme que celui qui a servi à générer la clé de contrôle imprimée sur le complexe. 35
8. Dispositif selon la revendication 7, **caractérisé par le fait que** le microprocesseur est supporté par une carte à puce enfichable dans le lecteur magnétique. 40
9. Dispositif selon l'une quelconque des revendications 7 à 8, **caractérisé par le fait que** le microprocesseur est enfermé dans une capsule inviolable. 45

## Claims

1. Complex intended to guarantee the tamper-resistance and authenticity of an object comprising: 50
  - a base support (1) solidly secured to the object (16) and on which are printed an identification code (3) and at least one authentication code (5, 6, 7), **characterized in that** it furthermore comprises: 55

- a protective foil (2), possibly opaque, partially covering the base support (1) so as to protect the authentication code (5, 6, 7) and able to be applied to the object (16) in such a way as to ensure the tamper-resistance thereof, and

- information (4) which relates to the object (16) itself and which is carried on the uncovered part of the base support (1).

2. Complex according to Claim 1, **characterized in that** the authentication code (5, 6, 7) printed on the base support is masked by an opaque layer of a scratch-off material (8, 9, 10).
3. Complex according to either of Claims 1 and 2, **characterized in that** the protective foil (2) constitutes proof of tamper-resistance of the protected object (16), guaranteeing that the latter has been neither opened nor used.
4. Complex according to any one of Claims 1 to 3, **characterized in that** it comprises an authentication code printed with a magnetic ink readable through the protective foil.
5. Complex according to Claim 4, **characterized in that** it comprises, **in that** part of the base support (1) not covered by the protective foil (2), a checking key generated by an algorithm on the basis, on the one hand, of the authentication code (5, 6, 7) of the complex, and, on the other hand, of an item of information specific to the protected object (16) appearing in a readable manner on the base support (1).
6. Device intended to guarantee the tamper-resistance and authenticity of an object, **characterized in that** it comprises complexes (1, 2) according to any one of Claims 1 to 5 and at least one file of links (36) containing the identification code or codes (3) of each complex in conjunction with its authentication code (5, 6, 7), as well as an authentication file (42) containing, in conjunction with the authentication code (5, 6, 7) of each complex, the information (4) which relates to the protected object (16) and is carried on the uncovered part of the base support (1) of the said complex.

7. Device intended to guarantee the tamper-resistance and authenticity of an object, **characterized in that** it comprises a complex (1, 2) according to Claim 5, and a magnetic reader built into which is a microprocessor executing the same algorithm as that which served to generate the checking key printed on the complex.

8. Device according to Claim 7, **characterized in that** the microprocessor is supported by a chip card which plugs into the magnetic reader.

9. Device according to either of Claims 7 and 8, **characterized in that** the microprocessor is enclosed in a tamper-resistant capsule.

#### Patentansprüche

1. Komplex zur Sicherstellung der Originalität und der Authentizität eines Objekts, umfassend:

- einen Basisträger (1), der mit dem Objekt (26) endgültig fest verbunden ist und auf den ein Identifizierungscode (3) und mindestens ein Authentifizierungscode (5, 6, 7) aufgedruckt sind,

**dadurch gekennzeichnet, dass** er außerdem umfasst:

- eine ggf. lichtundurchlässige Schutzfolie (2), die den Basisträger (1) teilweise bedeckt, um den Authentifizierungscode (5,6,7) zu schützen, und die auf das Objekt (16) aufgelegt werden kann, um die Originalität zu gewährleisten, und
- das Objekt (16) selbst betreffende Informationen (4), die auf dem nicht bedeckten Teil des Basisträgers (1) angeordnet sind.

2. Komplex nach Anspruch 1, **dadurch gekennzeichnet, dass** der auf den Basisträger aufgedruckte Authentifizierungscode (5,6,7) durch eine lichtundurchlässige Schicht aus einem abkratzbaren Werkstoff (8,9,10) maskiert ist.

3. Komplex nach einem der Ansprüche 1 und 2, **dadurch gekennzeichnet, dass** die Schutzfolie (2) einen Originalitätsbeweis für das geschützte Objekt (16) darstellt, der sicherstellt, dass dieser weder geöffnet noch benutzt wurde.

4. Komplex nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet, dass** er einen Authentifizierungscode aufweist, der mit einer magnetischen Druckfarbe aufgedruckt ist, die durch die Schutzfolie hindurch lesbar ist.

5. Komplex nach Anspruch 4, **dadurch gekennzeichnet, dass** er in dem nicht mit der Schutzfolie (2) bedeckten Teil des Basisträgers (1) einen Kontrollschlüssel aufweist, der durch einen Algorithmus auf der Basis einerseits des Authentifizierungscodes (5,6,7) des Komplexes und andererseits einer für das geschützte Objekt (16) spezifischen Informati-

on, die auf dem Basisträger (1) lesbar erscheint, erzeugt wird.

6. Vorrichtung zur Sicherstellung der Originalität und der Authentizität eines Objekts, **dadurch gekennzeichnet, dass** sie Komplexe (1,2) nach einem der Ansprüche 1 bis 5 und mindestens eine Linkdatei (36) aufweist, die den oder die Identifizierungscodes (3) jedes Komplexes in Zusammenhang mit seinem Authentifizierungscode (5,6,7) enthält, sowie eine Authentifizierungsdatei (42), die das geschützte Objekt (16) betreffende Informationen (4), die auf dem nicht bedeckten Teil des Basisträgers (1) des Komplexes vorgesehen sind, in Zusammenhang mit dem Authentifizierungscode (5,6,7) jedes Komplexes enthält.

7. Vorrichtung zur Sicherstellung der Originalität und der Authentizität eines Objekts, **dadurch gekennzeichnet, dass** sie einen Komplex (1,2) nach Anspruch 3 und einen Magnetleser aufweist, in den ein Mikroprozessor integriert ist, der denselben Algorithmus wie den, der zur Erzeugung des auf dem Komplex aufgedruckten Kontrollschlüssels gedient hat, herstellt.

8. Vorrichtung nach Anspruch 7, **dadurch gekennzeichnet, dass** der Mikroprozessor von einer in den Magnetleser einsteckbaren Chipkarte getragen wird.

9. Vorrichtung nach einem der Ansprüche 7 bis 8, **dadurch gekennzeichnet, dass** der Mikroprozessor in eine unverletzliche Kapsel eingeschlossen ist.



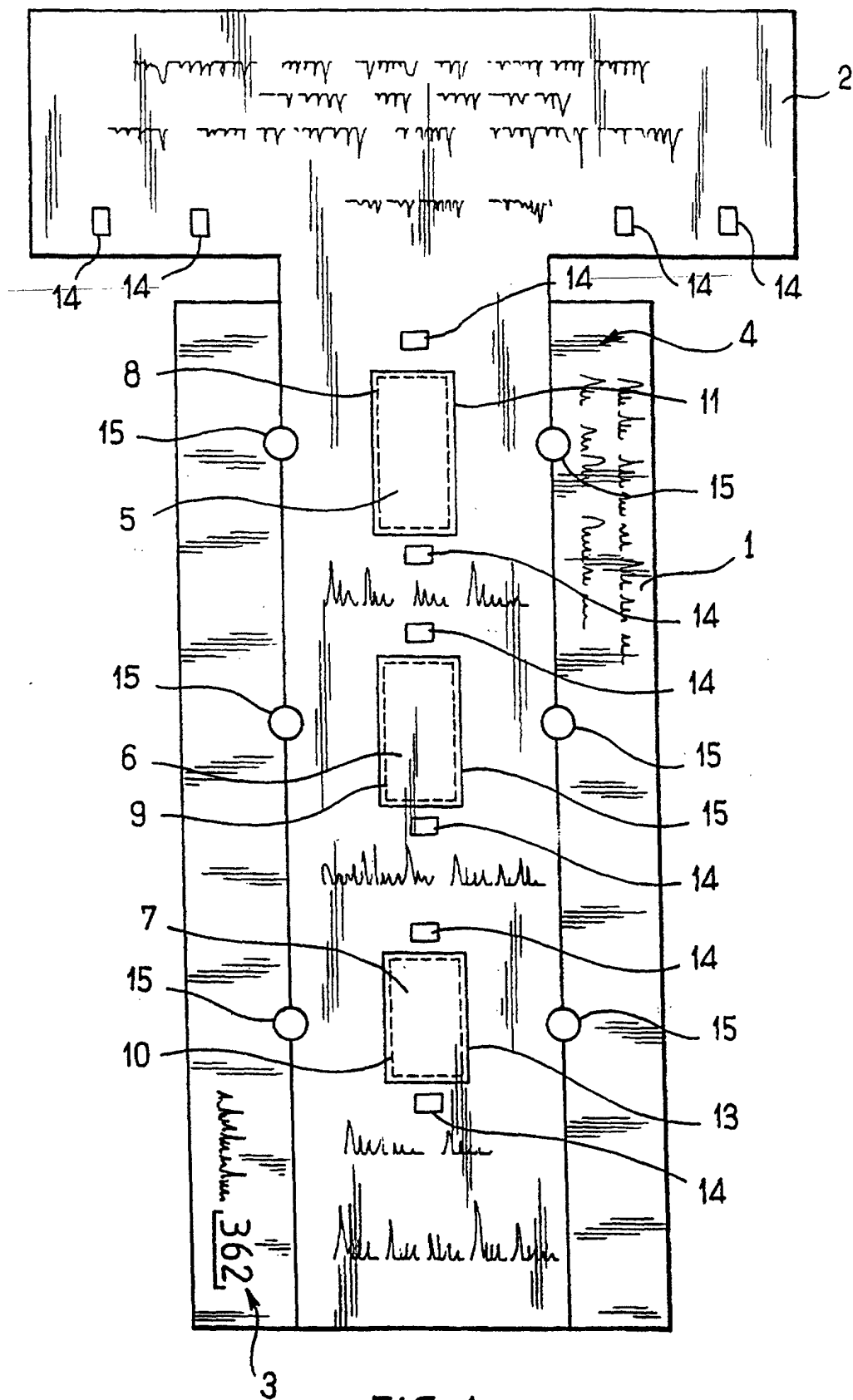


FIG. 1

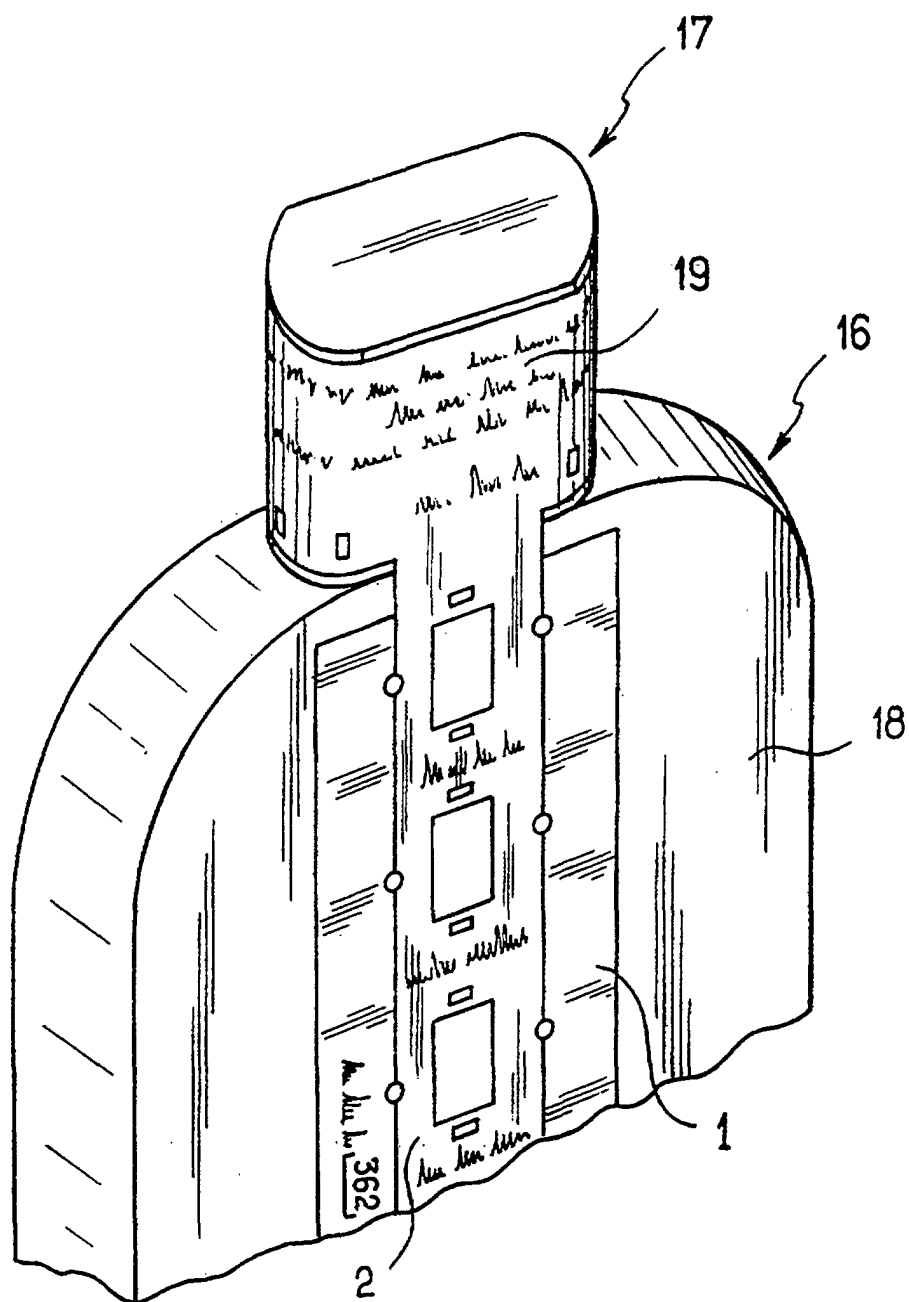


FIG. 2

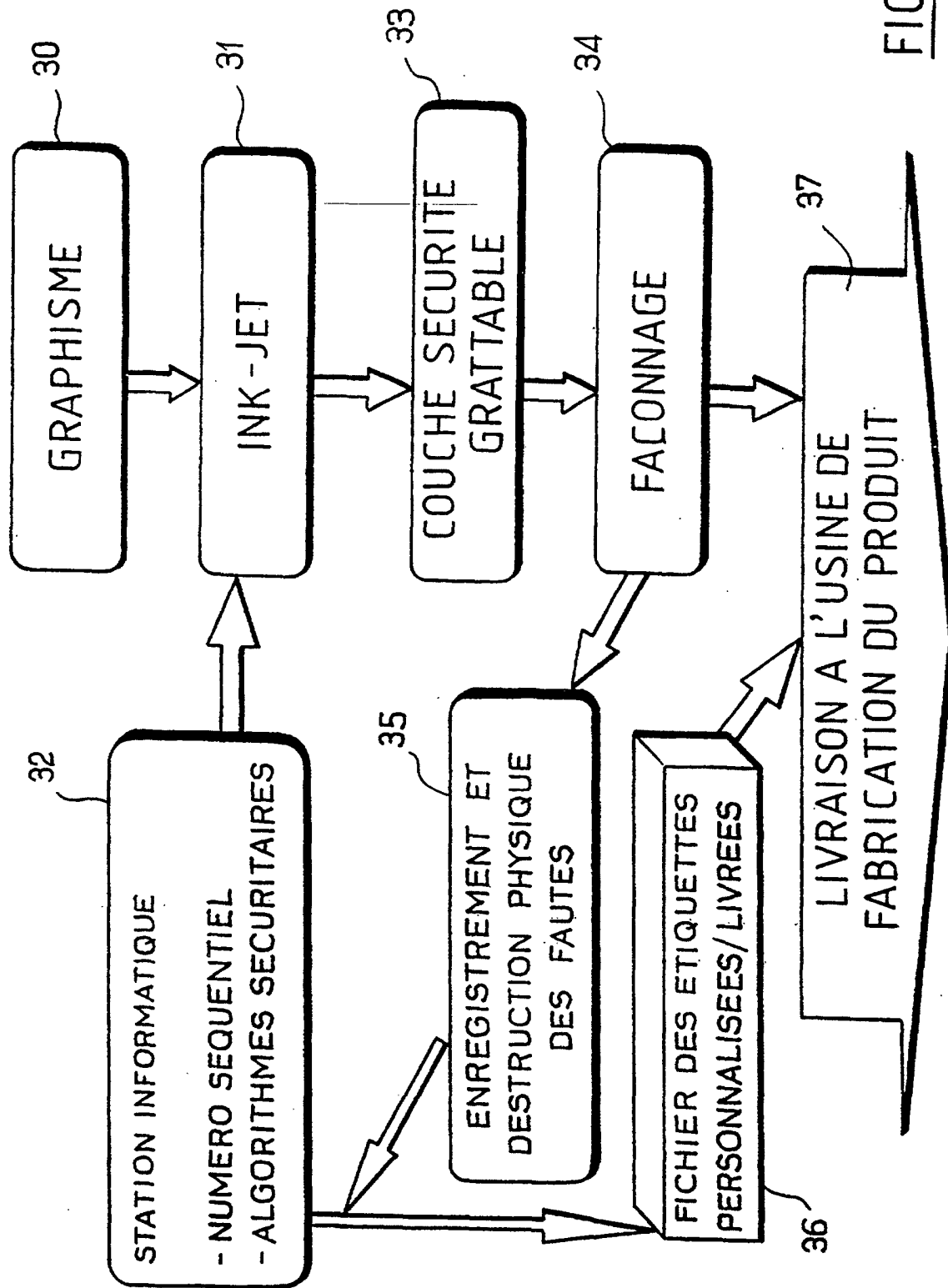


FIG. 3

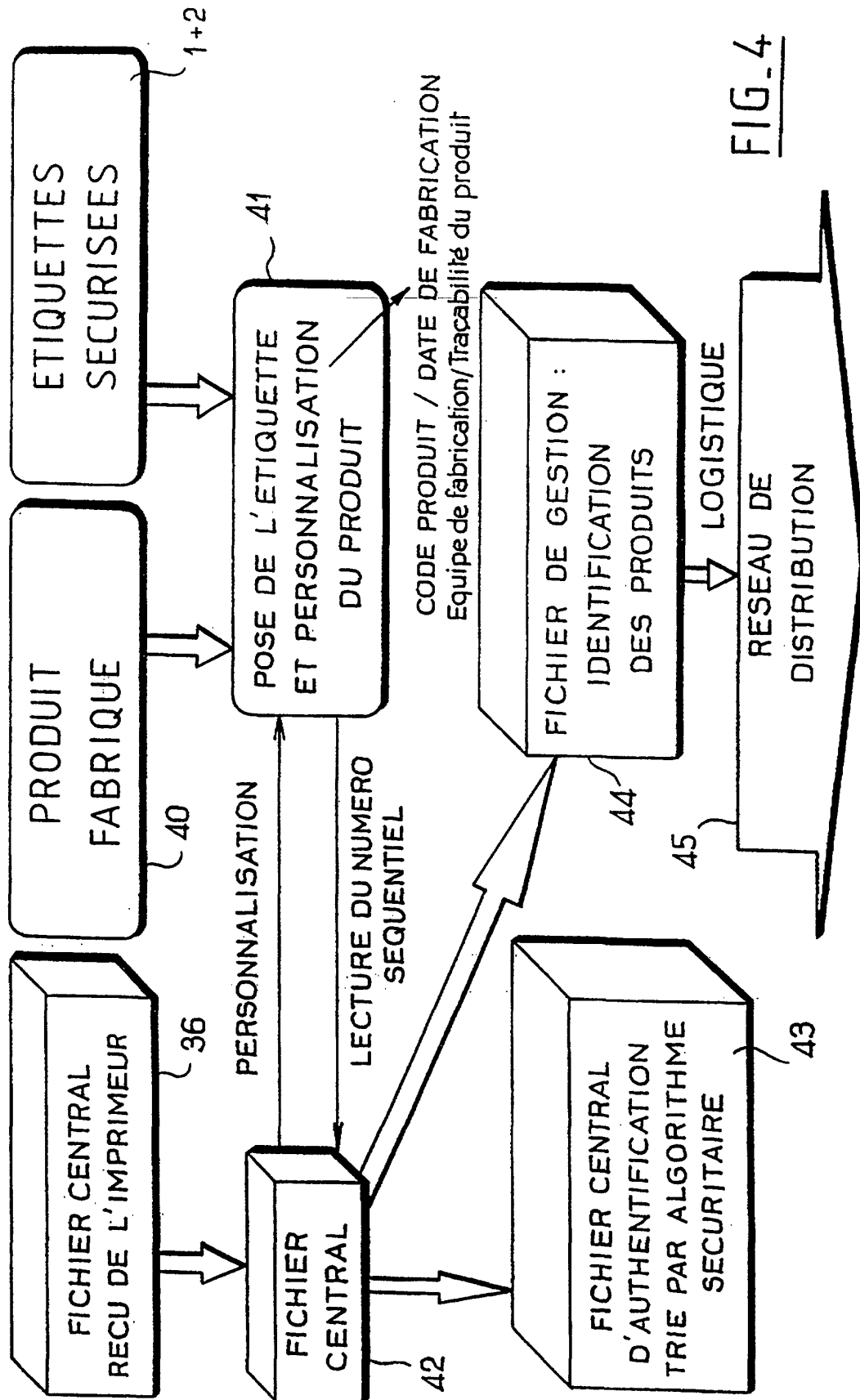
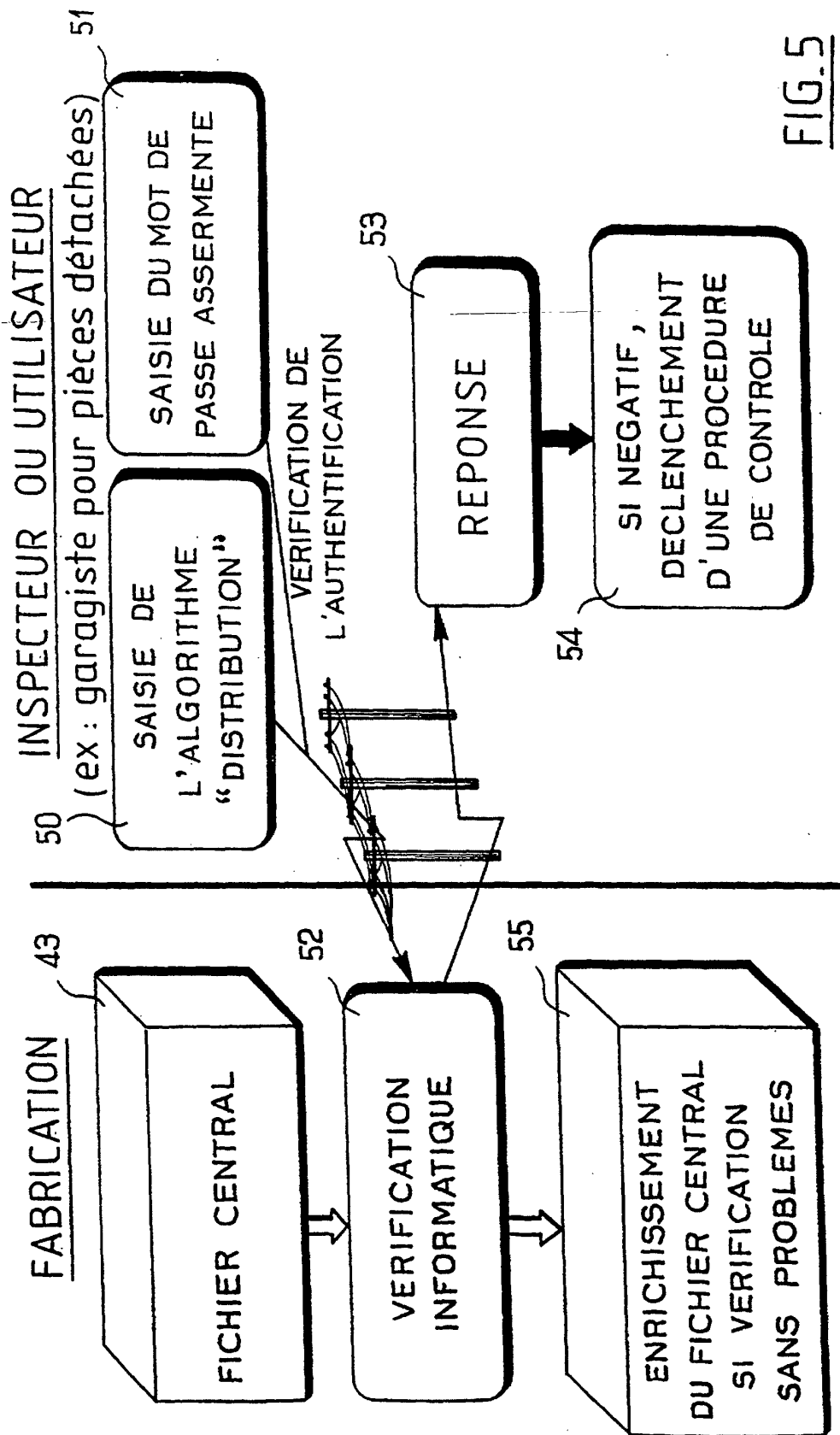


FIG. 4



**FIG. 5**

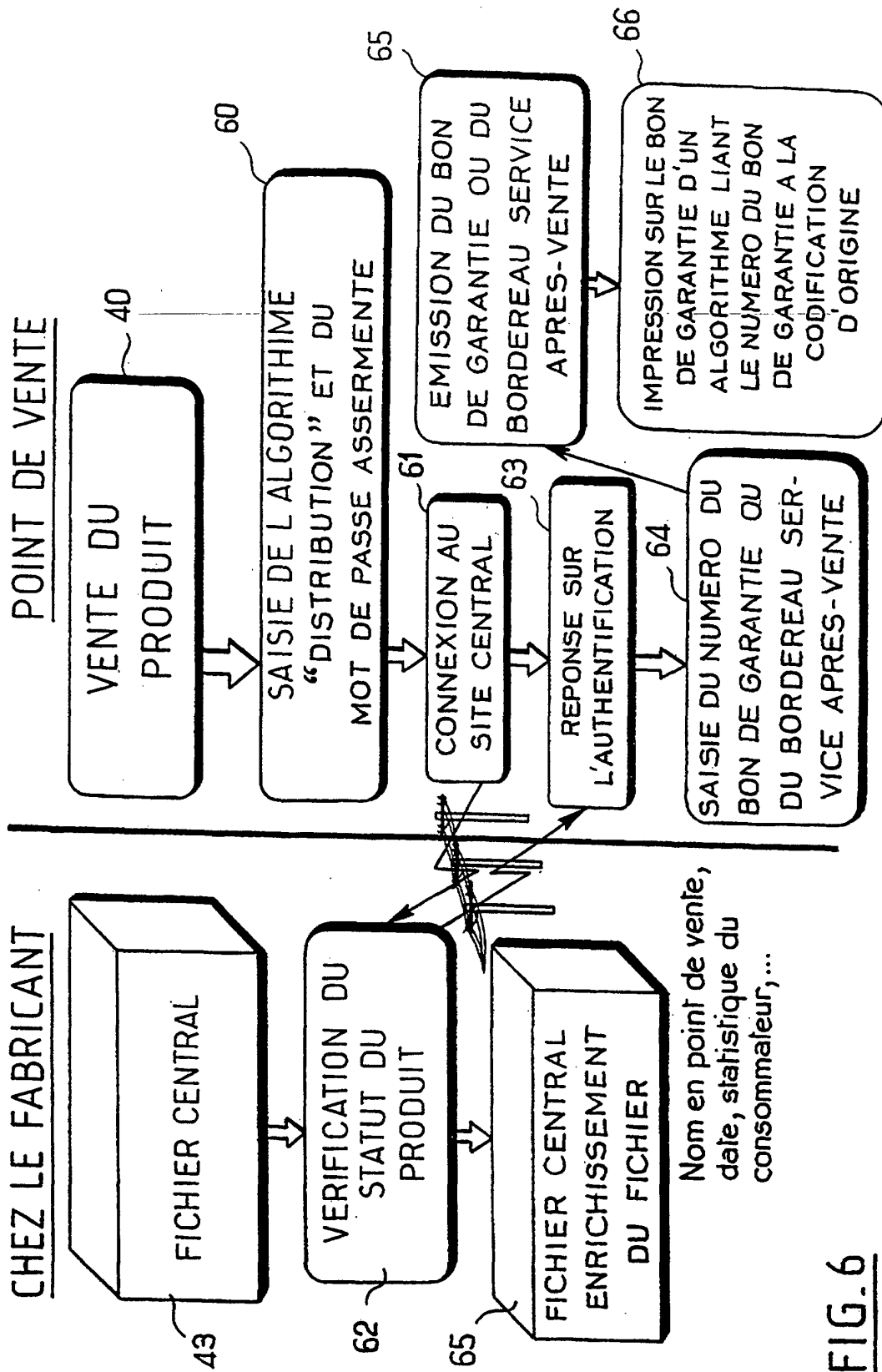
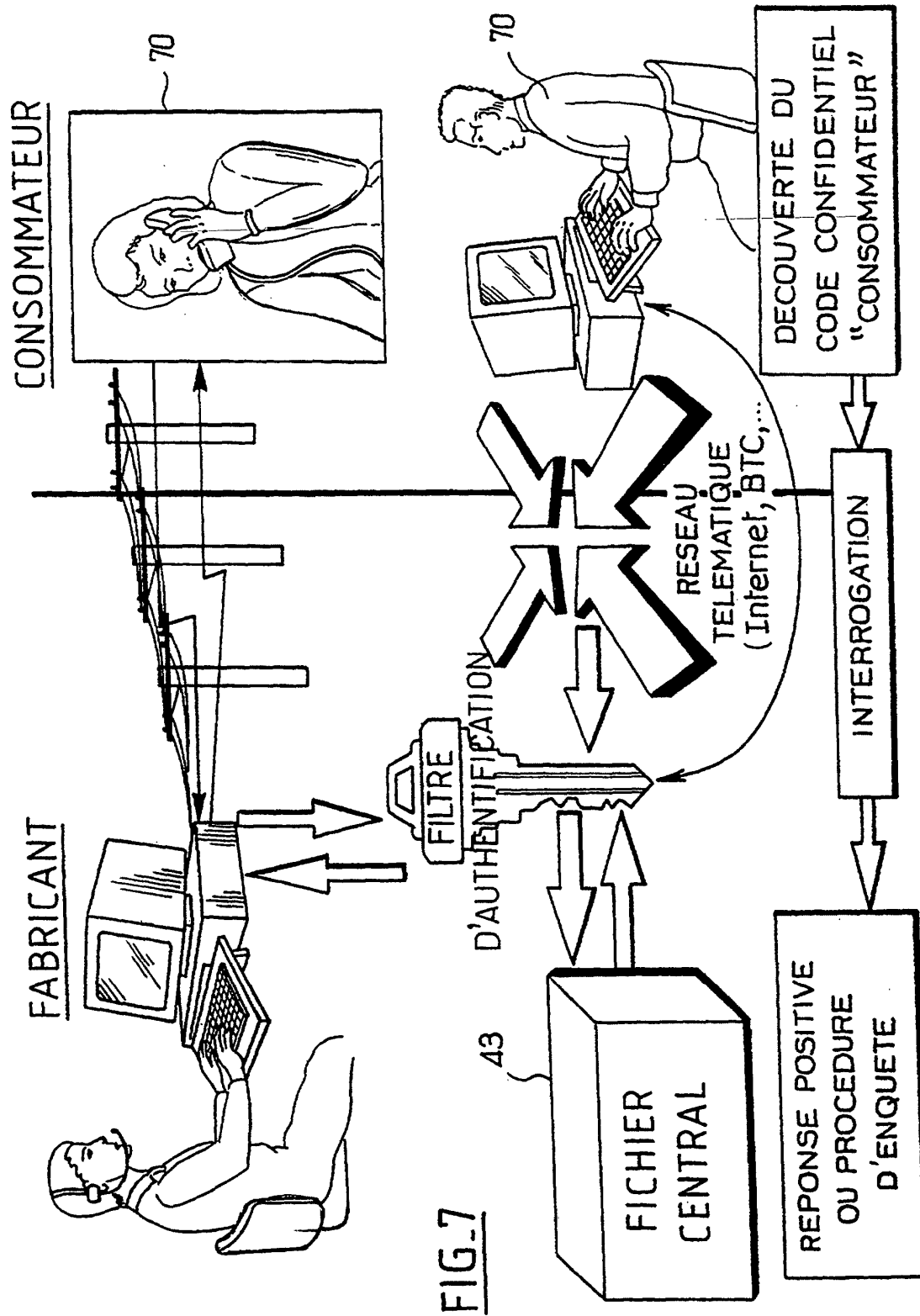


FIG. 6



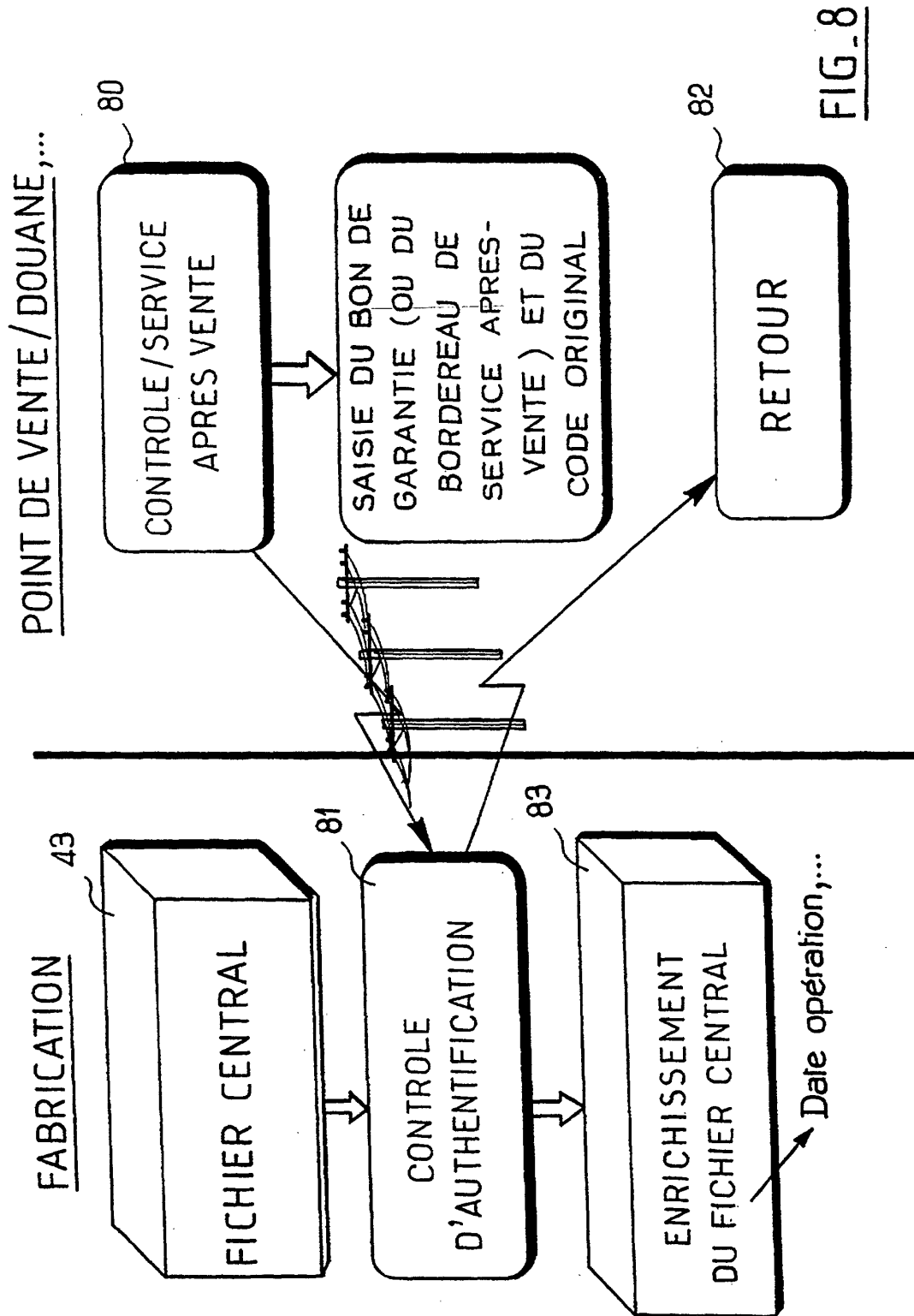


FIG. 8