(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 1 815 256 B1**

(12) **FASCICULE DE BREVET EUROPEEN**

(45) Date de publication et mention de la délivrance du brevet:
02.01.2013 Bulletin 2013/01

(21) Numéro de dépôt: **05818272.6**

(22) Date de dépôt: **22.11.2005**

(51) Int Cl.:
G07C 7/00 *(2006.01)* ***G01P 1/12*** *(2006.01)*
G07C 5/08 *(2006.01)*

(86) Numéro de dépôt international:
PCT/FR2005/002893

(87) Numéro de publication internationale:
WO 2006/053998 (26.05.2006 Gazette 2006/21)

(54) UNITÉ DE TACHYGRAPHE ÉLECTRONIQUE POUR VÉHICULE AUTOMOBILE

ELEKTRONISCHER TACHOGRAPH FÜR EIN KRAFTFAHRZEUG

ELECTRONIC SPEEDOGRAPH UNIT FOR MOTOR VEHICLE

(84) Etats contractants désignés:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR
Etats d'extension désignés:
AL BA HR MK YU

(30) Priorité: **22.11.2004 FR 0412379**

(43) Date de publication de la demande:
08.08.2007 Bulletin 2007/32

(73) Titulaire: **ACTIA Automotive**
31400 Toulouse (FR)

(72) Inventeurs:
- **MALBERTI, Laurent**
  F-31270 CUGNAUX (FR)
- **ROMON, Eric**
  F-31520 Ramonville Saint Agne (FR)
- **KUNEGEL, Jacques**
  31470 BONREPOS SUR AUSSONNELLE (FR)

(74) Mandataire: **Jacobson, Claude et al**
Cabinet Lavoix
2, Place d'Estienne d'Orves
75441 Paris Cedex 09 (FR)

(56) Documents cités:
EP-A- 0 592 166 **WO-A-02/31709**
US-A- 5 497 419 **US-B1- 6 556 905**

Il est rappelé que: Dans un délai de neuf mois à compter de la publication de la mention de la délivrance du brevet européen au Bulletin européen des brevets, toute personne peut faire opposition à ce brevet auprès de l'Office européen des brevets, conformément au règlement d'exécution. L'opposition n'est réputée formée qu'après le paiement de la taxe d'opposition. (Art. 99(1) Convention sur le brevet européen).

EP 1 815 256 B1

Description

[0001] L'invention concerne une unité d'un appareil de contrôle dit tachygraphe, destinée à être embarquée sur un véhicule automobile -notamment un véhicule de transport de marchandises ou de voyageurs- en vue de permettre le contrôle d'activités d'un conducteur du véhicule. A noter que le terme « conducteur » désigne une personne pouvant tour à tour exercer des activités de chauffeur ou de co-chauffeur (encore dit « convoyeur ») du véhicule. Le tachygraphe comprend, outre cette unité, au moins un capteur de mouvement du véhicule, relié à l'unité lorsque celle-ci est embarquée.

[0002] Un tachygraphe a notamment pour fonction d'enregistrer, de stocker, de produire, d'imprimer, et éventuellement d'échanger et d'afficher, des données, dites données conducteur, relatives aux activités d'un conducteur du véhicule, en vue de permettre un contrôle de ces activités par un contrôleur.

[0003] Les tachygraphes actuellement utilisés en Europe sont du type tachygraphe à disques graphiques, tels que celui décrit par US 4 782 691. Il s'agit d'instruments analogiques et mécaniques permettant de retranscrire des données conducteur sur un disque en papier au moyen d'un stylet.

[0004] Suivant une tendance généralisée dans le domaine de l'automobile, des tachygraphes électroniques ont par ailleurs été développés, dotés notamment de circuits à microprocesseurs pour le traitement et le stockage des données conducteur. L'introduction de l'électronique dans les tachygraphes a permis d'envisager la mise en oeuvre de nouveaux équipements au sein de l'unité de tachygraphe et la réalisation par celle-ci de nouvelles fonctions. Ainsi, par exemple, des études ont porté sur le remplacement des disques graphiques connus (et toujours utilisés...) par des cartes à puce électronique. Elles ont abouti à la conception d'unités de tachygraphe, telles que celle décrite par US 4 644 368, dotées de dispositifs lecteur/enregistreur de cartes à puce.

[0005] Les documents EP-A-0592 166 et WO-A-02/31709 décrivent d'autres exemples d'appareils enregistreur de données pour véhicules selon l'art antérieur.

[0006] Parallèlement, l'accent a été mis sur la garantie d'une plus grande sécurité dans le traitement des données, dans l'objectif d'éviter les fraudes. Une unité de tachygraphe dispose déjà, à cette fin, de protections mécaniques (boîtier renforcé éventuellement muni de sceaux de sécurité...). L'implantation de composants électroniques -et notamment de circuit(s) à microprocesseur(s) et de lecteur(s) de cartes à puce- dans l'unité de tachygraphe permet aujourd'hui d'envisager la mise en oeuvre de protections électroniques au sein de l'unité, telles que des mécanismes de sécurité cryptographiques.

[0007] L'invention vise à fournir un tachygraphe -et plus précisément une unité de tachygraphe- électronique sécurisé, dans lequel sont notamment garanties :

- l'authenticité (vérification de l'identité) mutuelle de l'unité de tachygraphe et de certains médias externes à l'unité (tels que le capteur de mouvement et les cartes à puce) avec lesquels l'unité est amenée à échanger des données ; à noter qu'un média est considéré comme étant externe à l'unité lorsqu'il n'est pas incorporé à la conception dans le boîtier sécurisé de l'unité et est indépendant ou détachable de l'unité,
- l'authenticité (vérification de l'origine) et l'intégrité des données échangées entre l'unité et certains médias externes à l'unité,
- l'intégrité, par signature électronique, de données déchargées depuis l'unité vers des dispositifs externes dit dispositifs de déchargement.

[0008] Pour mettre en oeuvre de tels mécanismes de sécurité, l'unité de tachygraphe doit conserver des secrets cryptographiques (clés de chiffrement privées ou secrètes, pour l'encryptage et le décryptage) et intégrer des algorithmes de chiffrement correspondants.

[0009] L'invention vise à fournir une unité de tachygraphe sécurisée, non seulement dotée de tels algorithmes et secrets cryptographiques, mais de plus et surtout dotée d'une protection électronique renforcée apte à offrir un niveau élevé de résistance aux attaques frauduleuses.

[0010] En effet, malgré les efforts déployés en la matière depuis de nombreuses années, aucune solution satisfaisante et fiable n'a pu être trouvée à ce problème. L'objectif est non seulement d'offrir un contrôle et une limitation de l'accès aux données gérées par l'unité, en lecture et/ou en écriture, mais aussi et surtout de garantir le respect de cette limitation en permettant de déceler toute falsification de ces données.

[0011] Un objectif de l'invention est de fournir une unité apte à résister fortement à une attaque menée à l'aide de moyens sophistiqués, qu'il s'agisse de moyens mis en oeuvre directement sur les circuits de l'unité ou à distance. L'invention vise en particulier à fournir une unité offrant un niveau de sécurité coté E3 FORT selon la méthodologie d'évaluation ITSEC.

[0012] Un autre objectif de l'invention est de fournir une unité de tachygraphe électronique plus performante également en terme de fonctionnalités.

[0013] En outre, l'invention vise à atteindre les objectifs précités à moindre coût, en proposant une unité de tachygraphe de faible prix de revient. En particulier, l'invention vise à fournir une unité de tachygraphe qui remplisse ces objectifs à partir de moyens, et notamment de composants électroniques, usuels et bon marché, ou éventuellement nouveaux mais de développement et de fabrication peu onéreux.

[0014] L'invention concerne une unité de tachygraphe destinée à être embarquée sur un véhicule automobile et à être reliée à au moins un capteur de mouvement du véhicule, laquelle unité comprend au moins une carte à microprocesseur(s), dite carte principale, pour le traite-

ment et le stockage de données, dites données tachygraphiques, comprenant au moins des données, dites données conducteur, relatives à des activités d'un conducteur dudit véhicule. L'unité de tachygraphe est par ailleurs adaptée pour effectuer des opérations, dites opérations de sécurité, mettant en oeuvre des algorithmes de chiffrement aux fins d'authentification d'au moins une partie des données tachygraphiques.

[0015] A noter que les termes « algorithmes de chiffrement » peuvent être employés pour désigner des algorithmes d'encryptage, des algorithmes de décryptage ou les deux. Par ailleurs, dans toute la suite, les termes « données de sécurité » désignent des données additionnelles mémorisées et/ou créées et/ou calculées et/ou utilisées... dans le cadre des opérations de sécurité. Les données de sécurité comprennent notamment des clés de chiffrement, des certificats délivrés par des organismes officiels habilités, des attributs de sécurité générés par une opération de sécurité pour une transmission de données, telles qu'une signature, une somme de contrôle -dite checksum-... Certaines de ces données, dites données secrètes, sont par définition secrètes : conservées au sein de l'unité de tachygraphe, elles doivent rester inaccessibles à toute personne non autorisée (l'unité de tachygraphe devant offrir un niveau de résistance fort aux attaques visant à obtenir ces données secrètes) ; il s'agit essentiellement de clés de chiffrement secrètes -symétriques- et de clés de chiffrement privées.

[0016] L'unité de tachygraphe selon l'invention est caractérisée en ce que :

- la carte principale comprend au moins un microprocesseur, dit microprocesseur principal, pour le traitement des données tachygraphiques,
- l'unité comprend au moins un circuit intégré physiquement protégé fournisseur de services cryptographiques, dit circuit CSP, distinct du(des) microprocesseur(s) principal(aux), circuit CSP dans lequel sont stockées au moins des données dites données de sécurité secrètes, ce circuit CSP étant adapté pour réaliser au moins une partie des opérations de sécurité lorsque l'unité est embarquée sur un véhicule.

[0017] A noter que le(s) circuit(s) CSP peu(ven)t être porté(s) par la carte principale ou par une ou plusieurs autre(s) carte(s).

[0018] Ainsi, l'invention consiste à sélectionner et séparer de l'ensemble des opérations mises en oeuvre par une unité de tachygraphe, au moins une partie des opérations relatives uniquement à la sécurité (opérations consistant à authentifier et/ou protéger certaines données au moyen d'algorithmes de chiffrement, dans le but final de garantir l'authenticité et l'intégrité des données conducteur), et à faire exécuter les opérations de sécurité sélectionnées par un circuit spécifique, physiquement protégé. Pour ce faire, dans ce circuit protégé sont stockées des données de sécurité secrètes. Peuvent également y être stockés les algorithmes de chiffrement et/ou des données de sécurité non secrètes (telles que des clés publiques) relatifs aux opérations de sécurité allouées audit circuit CSP.

[0019] Une telle architecture électronique permet de garantir un niveau de sécurité très élevé, jamais atteint à ce jour dans une unité de tachygraphe.

[0020] Comme il est expliqué ci-après, elle offre également la possibilité d'utiliser des composants électroniques usuels et peu onéreux.

[0021] Avantageusement et selon l'invention, le(s) circuit(s) CSP est(sont) dédié(s) essentiellement à la réalisation d'opérations de sécurité, le terme « essentiellement » signifiant que chaque circuit CSP est dédié à des opérations de sécurité et éventuellement à des opérations ponctuelles demandant une faible capacité de traitement et de stockage, telles que le stockage de données temporaires générées par le traitement de données tachygraphiques. Un circuit fournisseur de services cryptographiques usuel et peu onéreux, ayant une faible capacité de traitement et de stockage, peut ainsi être utilisé à titre de circuit CSP selon l'invention, compte tenu de ce que celui-ci est « déchargé » des fonctionnalités de l'unité de tachygraphe qui nécessitent plus de capacité.

[0022] Plus particulièrement, le(s) circuit(s) CSP est (sont) dédié(s) essentiellement à la réalisation de toutes les opérations de sécurité. Dès lors, le(s) microprocesseur(s) principal(aux) n'exécute(nt) aucune opération de sécurité. Il est donc possible d'utiliser, à titre de microprocesseur principal, un microprocesseur basique, non protégé et donc peu onéreux, tel que, par exemple, un calculateur usuellement utilisé dans le domaine automobile. Un tel calculateur classique possède une capacité de traitement et de stockage suffisante pour gérer l'ensemble des tâches (hors opérations de sécurité) dévolues à l'unité de tachygraphe.

[0023] Dans une version préférée de l'invention, l'unité de tachygraphe comprend un unique circuit CSP, essentiellement dédié à toutes les opérations de sécurité.

[0024] Avantageusement et selon l'invention, la carte principale de l'unité de tachygraphe comprend au moins une mémoire, dite mémoire d'application, associée à un microprocesseur principal, dans laquelle est stockée une application (un ou plusieurs programmes), dite application tachygraphique, qui peut être chargée dans ce microprocesseur principal pour le traitement des données tachygraphiques. Avantageusement et selon l'invention, ce microprocesseur principal est adapté pour pouvoir vérifier l'authenticité et l'intégrité d'au moins une partie de l'application tachygraphique à l'aide d'au moins une opération de sécurité réalisée par un circuit CSP de l'unité de tachygraphe.

[0025] En particulier, ledit microprocesseur principal intègre un programme de démarrage protégé, physiquement inscrit dans le microprocesseur et adapté pour, lors d'une opération visant à implémenter au moins une d'une application tachygraphique (première ou nouvelle) dans

l'unité, commander audit circuit CSP l'exécution d'au moins une opération de sécurité en vue de l'authentification de ladite application ou partie d'application tachygraphique, et ne commander l'enregistrement de cette application ou partie d'application tachygraphique dans la mémoire d'application que si elle est considérée par le circuit CSP comme étant authentique et intègre.

[0026] Le programme de démarrage étant inscrit en dur (dans le silicium) dans le microprocesseur principal, celui-ci ne peut pas être modifié. Ce qui garantit la commande par le microprocesseur principal et l'exécution par le circuit CSP de la(des) opération(s) de sécurité susmentionnée(s). L'application tachygraphique finalement stockée dans la mémoire d'application et utilisée par le (s) microprocesseur(s) principal(aux) est donc nécessairement authentique et intègre, c'est-à-dire conçue et implémentée par un organisme habilité, dans un environnement sécurisé, selon les spécifications imposées par les règles et normes.

[0027] En outre, il est de préférence prévu que l'application tachygraphique stockée dans la mémoire d'application soit elle-même adaptée pour, lorsqu'elle est chargée dans le microprocesseur principal pour le traitement des données tachygraphiques, commander périodiquement au circuit CSP associé l'exécution d'au moins une opération de sécurité en vue de sa propre authentification.

[0028] Avantageusement et selon l'invention, chaque circuit CSP est relié à un microprocesseur principal, lesdits circuit CSP et microprocesseur principal associés étant adaptés pour fonctionner selon une relation maître/esclave dans laquelle le microprocesseur principal est le maître et le circuit CSP est l'esclave.

[0029] Ainsi, toutes les opérations de sécurité exécutées par un circuit CSP le sont à la demande du microprocesseur principal associé, qui, pour ce faire, transmet au circuit CSP des données à authentifier assorties d'au moins une commande d'exécution d'une opération de sécurité correspondante.

[0030] L'unité de tachygraphe selon l'invention comprend un dispositif lecteur/enregistreur de cartes à puce, dites cartes tachygraphiques, apte à recevoir au moins deux cartes tachygraphiques en parallèle.

[0031] Dans une version préférée de l'invention, l'unité de tachygraphe comprend également une interface de connexion, dite interface de carte tachygraphique, pour une communication sans fil (et notamment à distance) de l'unité avec un dispositif lecteur/enregistreur de cartes tachygraphiques externe à l'unité (dans sa version la plus simple, ce dispositif externe est adapté pour ne recevoir qu'une seule carte tachygraphique à la fois).

[0032] Quatre types de cartes tachygraphiques sont prévues, chaque carte tachygraphique appartenant à l'un de ces types : les cartes de conducteur, les cartes de contrôleur, les cartes d'entreprise et les cartes d'atelier. Chaque type de carte tachygraphique ouvre droit d'une part à un accès restreint à certaines données prédéterminées stockées dans l'unité, et d'autre part à l'exécution de certaines opérations prédéterminées selon le type de carte tachygraphique. L'insertion d'une carte tachygraphique dans le dispositif lecteur/enregistreur de cartes (qu'il s'agisse du dispositif de l'unité -dit dispositif intégré- ou d'un dispositif externe apte à communiquer avec l'unité) permet d'ouvrir une session de fonctionnement de l'unité correspondant au type de la carte insérée.

[0033] Conformément aux objectifs fixés, toute carte tachygraphique insérée dans le dispositif lecteur/enregistreur de cartes (intégré ou externe) doit pouvoir être authentifiée, de même que les données échangées entre ladite carte tachygraphique et l'unité de tachygraphe.

[0034] A cette fin, selon l'invention, le dispositif lecteur/enregistreur est contrôlé par au moins un microprocesseur principal de l'unité, auquel est associé un circuit CSP. Ce microprocesseur principal (ou éventuellement ces microprocesseurs principaux) est adapté pour commander audit circuit CSP l'exécution d'opérations de sécurité en vue de l'authentification mutuelle de l'unité et d'une carte tachygraphique présente dans le dispositif lecteur/enregistreur de cartes (intégré ou externe), et n'autoriser l'ouverture d'une session de fonctionnement correspondante que si l'unité et la carte tachygraphique sont considérées comme étant authentiques.

[0035] Une carte de conducteur authentifiée donne ainsi accès à une session de fonctionnement dite session de conducteur ; une carte d'atelier authentifiée donne accès à une session de fonctionnement dite session d'atelier ; une carte de contrôleur authentifiée donne accès à une session de fonctionnement dite session de contrôleur ; une carte d'entreprise authentifiée donne accès à une session de fonctionnement dite session d'entreprise.

[0036] Cette authentification mutuelle entre carte tachygraphique et unité est de préférence exécutée dès qu'une carte est insérée dans le dispositif lecteur/enregistreur de cartes (s'agissant notamment du dispositif intégré). A cette fin, le microprocesseur principal est adapté pour surveiller les insertions et retraits de carte dans le dispositif lecteur/enregistreur et déclencher les opérations de sécurité susmentionnées dès qu'une insertion d'une carte tachygraphique dans le dispositif lecteur/enregistreur est détectée.

[0037] L'ouverture d'une session de fonctionnement permet la réalisation d'opérations, dont la nature dépend du type de la session. Certaines de ces opérations peuvent conduire à des échanges de données entre carte tachygraphique et unité. A chaque échange de données entre l'unité de tachygraphe et une carte tachygraphique présente dans le dispositif lecteur/enregistreur de cartes (intégré ou externe) et préalablement authentifiée, le microprocesseur principal est adapté pour commander au circuit CSP l'exécution d'au moins une opération de sécurité en vue de l'authentification desdites données, et ne traiter les données échangées que si elles sont considérées comme étant authentiques et intègres.

[0038] En particulier, le microprocesseur principal est adapté pour :

- lorsque des données (notamment des données tachygraphiques) sont reçues par l'unité depuis ladite carte tachygraphique, commander au circuit CSP l'exécution d'au moins une opération de sécurité en vue de l'authentification des données reçues, et ne traiter lesdites données que si elles sont considérées par le circuit CSP comme étant authentiques et intègres,
- lorsque des données doivent être transmises par l'unité à ladite carte tachygraphique, commander au circuit CSP l'exécution d'au moins une opération de sécurité en vue de la protection de l'intégrité des données à transmettre. La carte tachygraphique est par ailleurs adaptée pour exécuter au moins une opération de sécurité en vue d'authentifier les données transmises, et ne traiter lesdites données que si elle les considère comme étant authentiques et intègres.

[0039] L'unité de tachygraphe doit par ailleurs pouvoir authentifier le capteur de mouvement avec lequel elle communique lorsqu'elle est embarquée sur un véhicule, ainsi que les données, dites données de mouvement, qu'elle reçoit dudit capteur. A noter que les données de mouvement sont des données tachygraphiques.

[0040] Pour sa liaison au capteur de mouvement, l'unité de tachygraphe comprend une interface de connexion, dite interface de capteur. A noter que cette liaison est de préférence filaire, auquel cas l'interface de capteur est constituée d'un ou plusieurs connecteur(s). Mais il n'est pas exclu que cette liaison soit sans fil et que l'interface de capteur comprenne (éventuellement en combinaison avec un connecteur) un dispositif émetteur-récepteur d'ondes électromagnétiques.

[0041] Par ailleurs, selon l'invention, la carte principale de l'unité comprend au moins un microprocesseur principal relié à ladite interface de capteur et auquel est associé un circuit CSP, ledit microprocesseur principal étant adapté pour commander audit circuit CSP l'exécution d'opérations de sécurité en vue d'une part de l'authentification mutuelle du capteur de mouvement et de l'unité et d'autre part de l'authentification des données de mouvement reçues du capteur de mouvement par l'unité, et ne traiter les données de mouvement reçues que si le capteur de mouvement et l'unité sont considérés comme étant authentiques et si les données reçues sont considérées comme étant authentiques et intègres.

[0042] En particulier, le microprocesseur principal est adapté pour :

- dans le cadre d'une opération initiale dite opération d'appariement d'un capteur de mouvement et de l'unité de tachygraphe, commander au circuit CSP l'exécution d'au moins une opération de sécurité en vue de l'authentification mutuelle du capteur et de l'unité, et n'autoriser un échange ultérieur de données entre ledit capteur et l'unité que si ces derniers sont considérés comme étant authentiques,
- dans le cadre d'une opération périodique, dite opération de contrôle des données de mouvement, commander au circuit CSP l'exécution d'au moins une opération de sécurité en vue de l'authentification de données, dites données de contrôle, échangées entre le capteur et l'unité dans le cadre de cette opération de contrôle, et n'autoriser le traitement des données de mouvement reçues par l'unité sur une période écoulée que si lesdites données de contrôle sont considérées comme étant authentiques et intègres. En d'autres termes, pour garantir l'authenticité et l'intégrité des données de mouvement, seules sont vérifiées l'authenticité et l'intégrité des données de contrôle.

[0043] Pour une plus grande sécurité, l'opération d'appariement ne peut être mise en oeuvre que si une carte tachygraphique d'atelier authentique et authentifiée est présente dans le dispositif lecteur/enregistreur de cartes intégré à l'unité. En d'autres termes, le(s) microprocesseur(s) principal(aux) de l'unité est(sont) adapté(s) pour n'autoriser l'exécution d'une opération d'appariement que dans le cadre d'une session d'atelier (qui ne peut être ouverte que par l'authentification d'une carte d'atelier).

[0044] Avantageusement et selon l'invention, l'unité de tachygraphe comprend également une interface de connexion, dite interface de déchargement, pour la communication de l'unité avec un dispositif externe dit dispositif de déchargement, notamment apte à mémoriser des données tachygraphiques. L'interface de déchargement peut comprendre un connecteur, en vue d'une connexion filaire du dispositif de déchargement avec l'unité, et/ou un dispositif émetteur/récepteur d'ondes électromagnétiques, en vue d'une communication sans fil entre l'unité et un dispositif de déchargement éventuellement distant.

[0045] Selon l'invention, une opération de déchargement de données ne peut être mise en oeuvre, sur commande d'un utilisateur, que si une carte tachygraphique de contrôleur, d'atelier ou d'entreprise (à l'exclusion d'une carte de conducteur) authentique et authentifiée est présente dans le dispositif lecteur/enregistreur de cartes (intégré ou externe). A cette fin, le(s) microprocesseur(s) principal(aux) est(sont) adapté(s) pour n'autoriser l'exécution d'une opération de déchargement de données vers un dispositif de déchargement « connecté » à l'unité (connexion filaire ou sans fil) par l'intermédiaire de l'interface de déchargement, que dans le cadre d'une session de contrôleur ou d'atelier ou d'entreprise (ouverte par l'authentification d'une carte correspondante).

[0046] A noter que les données dont le déchargement est autorisé peuvent différer selon la session de fonctionnement en cours.

[0047] Avantageusement et selon l'invention, les données tachygraphiques déchargées sont assorties d'un attribut de sécurité, tel qu'une signature électronique, en vue de leur authentification ultérieure par le dispositif de

déchargement ou par un autre outil. Le microprocesseur principal est également adapté pour, dans le cadre d'une opération de déchargement de données, commander au circuit CSP l'exécution d'au moins une opération de sécurité en vue de la protection des données à décharger.

[0048] Par ailleurs, l'unité comprend également avantageusement une interface de connexion, dite interface d'étalonnage, comprenant au moins un connecteur, pour la communication de l'unité avec un dispositif externe dit dispositif d'étalonnage, en vue de l'étalonnage de l'unité.

[0049] Selon l'invention, une opération d'étalonnage ne peut être mise en oeuvre, sur commande d'un utilisateur, au moyen d'un dispositif d'étalonnage connecté à l'unité par l'intermédiaire de l'interface d'étalonnage, que si une carte tachygraphique d'atelier authentique et authentifiée est présente dans le dispositif lecteur/enregistreur de cartes intégré à l'unité. A cette fin, le(s) microprocesseur(s) principal(aux) est(sont) adapté(s) pour n'autoriser l'exécution d'une opération d'étalonnage que dans le cadre d'une session d'atelier (ouverte par l'authentification d'une carte d'atelier).

[0050] Lors d'une opération d'étalonnage, des données dites données d'étalonnage sont transmises à l'unité par le dispositif d'étalonnage. Les données d'étalonnage mémorisées dans l'unité en fin d'opération d'étalonnage sont des données tachygraphiques.

[0051] Avantageusement et selon l'invention, un microprocesseur principal de l'unité est adapté pour surveiller les insertions et retraits de carte dans le dispositif lecteur/enregistreur de cartes (intégré ou externe) et pour, dès qu'un retrait d'une carte tachygraphique du dispositif lecteur/enregistreur est détecté, interrompre toute opération en cours dans la session de fonctionnement correspondante. En particulier, sont ainsi interrompues les opérations en cours d'appariement de capteur, de mise à jour de l'application tachygraphique, d'étalonnage, de déchargement de données tachygraphique et bien entendu de lecture/écriture sur la carte tachygraphique (qui n'est plus connectée...).

[0052] Dans une version préférée de l'invention :

- la carte principale comprend un unique microprocesseur principal pour le traitement des données tachygraphiques, auquel sont reliés un circuit d'alimentation électrique alimenté de façon permanente par une source électrique permanente du véhicule, une mémoire de masse, dite mémoire d'application, de type électronique et non volatile -et notamment de type flash-pour le stockage d'au moins une application tachygraphique, une mémoire de masse, dite mémoire de données, de type électronique et non volatile -et notamment de type flash- pour le stockage de données tachygraphiques et éventuellement d'autres données à l'exclusion de données de sécurité secrètes (les deux mémoires précédemment définies pouvant être deux mémoires distinctes ou une seule et même mémoire), une horloge temps réel calendaire, un connecteur de capteur et un (unique) connecteur, dit connecteur de déchargement/étalonnage, pour la connexion à l'unité d'un dispositif externe d'étalonnage ou d'un dispositif externe de déchargement, un dispositif lecteur/enregistreur tel que précédemment défini,
- l'unité comprend un unique circuit CSP, dédié à la réalisation de toutes les opérations de sécurité, lesdits microprocesseur principal et circuit CSP étant reliés et adaptés pour fonctionner selon une relation maître/esclave dans laquelle le microprocesseur principal est le maître et le circuit CSP est l'esclave,
- l'unité comprend également une imprimante, un écran d'affichage, un dispositif de saisie de données par un utilisateur (tel qu'un clavier).

[0053] L'invention concerne également une unité de tachygraphe caractérisée en combinaison par tout ou partie des caractéristiques mentionnées ci-dessus et ci-après.

[0054] L'invention s'étend à un véhicule automobile équipé d'une telle unité de tachygraphe.

[0055] D'autres buts, caractéristiques et avantages de l'invention apparaîtront à la lecture de la description suivante qui se réfère aux figures annexées représentant des modes de réalisation préférentiels de l'invention, donnés uniquement à titre d'exemples non limitatifs, et dans lesquelles :

- la figure 1 est une vue en perspective d'une unité de tachygraphe selon l'invention,
- la figure 2 est une vue éclatée en perspective d'une unité de tachygraphe selon l'invention,
- la figure 3 est un schéma synoptique illustrant l'architecture de cette unité de tachygraphe et l'organisation de ses différents composants,
- la figure 4 est un organigramme illustrant le déroulement d'une opération de sécurité selon l'invention.

[0056] L'unité de tachygraphe 1 selon l'invention comprend, au sein d'un boîtier sécurisé 2 renforcé (formé de plusieurs éléments 2a, 2b, 2c) et doté de sceaux de sécurité 50 :

- une carte principale 3 à microprocesseur(s), qui porte un microprocesseur principal 4, tel que ceux usuellement utilisés dans le domaine automobile ; en variante, ladite carte porte un groupe de microprocesseurs en parallèle en vue d'assurer une redondance, ou une pluralité de microprocesseurs indépendants ou reliés en série qui se partagent les fonctionnalités du tachygraphe ; la carte principale 3 porte également un circuit CSP 20 fournisseur de services cryptographiques, relié au microprocesseur principal 4 selon une relation maître/esclave dans laquelle le microprocesseur principal 4 est le maître et le circuit CSP 20 est l'esclave ; un tel circuit CSP est physiquement protégé ; il possède à cette fin des caractéristiques non seulement physiques

mais aussi fonctionnelles (mémoire apte à disperser les secrets qu'il renferme...) garantissant son inviolabilité ; le circuit CSP 20 est par exemple un microprocesseur CSP similaire à ceux employés pour les cartes bancaires ; le circuit CSP 20 intègre une mémoire protégée dans laquelle sont stockés des algorithmes de chiffrement, des données de sécurité secrètes (clés privées et clés de session) et éventuellement d'autres données de sécurité (clés publiques..., ces autres données de sécurité pouvant en variante être stockées dans une mémoire non protégée de l'unité), en vue de l'exécution d'opérations de sécurité,

- une mémoire de masse flash 5, dite mémoire d'application, reliée au microprocesseur principal 4, et dans laquelle est stockée une application tachygraphique permettant de réaliser toutes les fonctionnalités du tachygraphe à l'exclusion d'au moins une partie des opérations de sécurité, et de préférence à l'exclusion de toutes les opérations de sécurité à mettre en oeuvre pour garantir un niveau élevé de résistance aux attaques frauduleuses ; à noter toutefois que l'application tachygraphique intègre des commandes permettant de déclencher l'exécution des opérations de sécurité ; la mémoire d'application 5 est du type non volatile,
- un circuit d'alimentation électrique 6 relié de façon permanente à une source électrique permanente du véhicule en vue d'alimenter le microprocesseur principal 4 en permanence quelle que soit la phase d'exploitation du véhicule en cours (hors contact, après contact, moteur arrêté, moteur tournant, véhicule à l'arrêt, véhicule roulant...),
- une horloge temps réel calendaire 7 (date et heure) reliée au microprocesseur principal 4, et qui dispose de préférence d'une batterie de secours,
- un dispositif double 8 lecteur/enregistreur de cartes tachygraphiques à puce, piloté par le microprocesseur principal 4 et apte à recevoir deux cartes tachygraphiques en parallèle. Le dispositif dispose de deux blocs 81, 82 sensiblement identiques, comprenant chacun :

  ■ une interface mécanique (à fente, tiroir, chariot coulissant...) de réception d'une carte tachygraphique, dotée d'un mécanisme motorisé commandé pour le déplacement d'une carte 60 entre une position d'introduction/retrait et une position verrouillée de lecture/écriture,

  ■ un connecteur permettant la liaison entre le microprocesseur principal 4 de l'unité et la puce 61 d'une carte tachygraphique présente en position verrouillée de lecture/écriture,

  ■ au moins un organe de détection de carte en position verrouillée de lecture/écriture, apte à transmettre un signal au microprocesseur principal 4 lorsqu'une carte est détectée en position verrouillée de lecture/écriture,

- un dispositif 16 émetteur/récepteur d'ondes électromagnétiques, relié au microprocesseur principal 4 et formant une interface de connexion, dite interface de cartes, pour la communication sans fil de l'unité avec un dispositif lecteur/enregistreur de cartes tachygraphiques externe à l'unité,
- un dispositif 14 émetteur/récepteur d'ondes électromagnétiques, relié au microprocesseur principal 4 et réalisant une interface de connexion de l'unité 1 avec un dispositif de déchargement distant ; en variante, un seul et même dispositif émetteur/récepteur réalise une interface de communication à la fois avec un dispositif lecteur/enregistreur de cartes et avec un dispositif de déchargement de données distants,
- un écran d'affichage 9, avec rétro-éclairage, piloté par le microprocesseur principal 4,
- une imprimante 10 pilotée par le microprocesseur principal 4,
- un dispositif 11 de saisie de données par un utilisateur, piloté par le microprocesseur principal 4 et comprenant un clavier à touches et/ou un écran tactile,
- un connecteur 12 de capteur relié au microprocesseur principal 4, réalisant une interface de connexion de l'unité 1 avec un capteur de mouvement en vue de la réception de données de mouvement du véhicule,
- un connecteur 13 de déchargement/étalonnage relié au microprocesseur principal 4, réalisant une interface de connexion de l'unité 1 avec un dispositif d'étalonnage ou un dispositif de déchargement, en vue de la réception de données d'étalonnage (envoyées par le dispositif d'étalonnage) ou du déchargement (à destination du dispositif de déchargement) de données tachygraphiques,
- une pluralité de connecteurs 15 reliés au microprocesseur principal 4, pour la connexion de l'unité à certains calculateurs ou contacteurs du véhicule tels que le calculateur de vitesse, le compteur kilométrique, le calculateur de régime moteur, le réseau CAN de calculateurs du véhicule, en vue de la transmission de données entre l'unité et ces calculateurs, ainsi qu'un autre connecteur 15 pour la connexion du microprocesseur principal 4 de l'unité à un indicateur d'avertissement (signalement lumineux et/ou sonores),
- une mémoire de masse flash 17 de type non volatile, dite mémoire de données, reliée au microprocesseur principal 4 et dans laquelle sont stockées les données tachygraphiques, des données dites données de fonctionnement (taux d'éclairage de l'écran 9, zone image des tickets à imprimer par l'imprimante 10...) et des données dites données annexes (aléas, données temporaires...), et éventuellement des données de sécurité à condition qu'elles ne soient pas secrètes (clés publiques par exemple).

[0057] Outre l'unité 1, le tachygraphe comprend un capteur de mouvement du véhicule, des câbles de liaison permettant de relier le capteur de mouvement et le connecteur de capteur 12 de l'unité embarquée. Le capteur de mouvement est notamment formé d'un élément de détection de mouvement, d'un microprocesseur (auquel est relié l'élément de détection) et d'un connecteur pour la connexion du microprocesseur du capteur à l'unité embarquée.

[0058] L'unité de tachygraphe a pour fonction principale le traitement de données conducteur, parmi lesquelles on peut citer :

- la vitesse instantanée, la distance parcourue entre deux arrêts, ces données étant calculées à partir des données de mouvement relevées et transmises par le capteur de mouvement,
- les activités du conducteur (conduite -lorsque le conducteur conduit le véhicule-, travail, pause/repos, disponibilité -lorsque le « conducteur », c'est-à-dire le titulaire de la carte tachygraphique, est co-chauffeur), ces données étant, selon les cas, imposées automatiquement (par l'application tachygraphique) ou saisies manuellement par le conducteur au moyen du clavier 11,
- le temps de chaque activité,
- le lieu de début et de fin des périodes journalières de travail, ces données étant saisies manuellement par le conducteur,
- les conditions particulières (« hors champ », trajet en ferry/train), ces données étant saisies manuellement par le conducteur.

[0059] Selon l'invention, les fonctions attribuées au microprocesseur principal concernent essentiellement des fonctions de calcul portant sur les données conducteur, des fonctions plus générales de gestion de l'ensemble des données tachygraphiques (données conducteur, données de mouvement, données contrôleur, données d'étalonnage, données d'entreprise...) et des fonctions de pilotage des divers organes de l'unité embarquée. Parmi ces fonctions, on peut citer :

- la génération et le traitement de données conducteur, et notamment :
  - ■ le traitement des données de mouvement du véhicule (émanant du capteur de mouvement et reçues par l'intermédiaire du connecteur de capteur), et en particulier le calcul de la vitesse et de la distance parcourue, la mesure du temps,
  - ■ le suivi des activités du conducteur, le suivi de la situation de conduite,
  - ■ le traitement des données conducteur saisies manuellement par le conducteur (telles que le lieu de début et de fin des périodes journalières de travail, les activités du conducteur et les conditions particulières),
- la lecture de données stockées dans les mémoires d'application 5 et de données 17, l'enregistrement et le stockage de données dans ces mémoires,
- le contrôle du dispositif 8 lecteur/enregistreur de cartes tachygraphiques en vue notamment de la surveillance des insertions et retraits de carte, de la lecture des cartes tachygraphiques, de l'enregistrement et le stockage de données sur les cartes tachygraphiques, et éventuellement de l'actionnement des mécanismes de déplacement de carte,
- le contrôle de l'écran d'affichage 9,
- le contrôle de l'imprimante 10,
- le traitement des données saisies manuellement par le conducteur au moyen du clavier 11,
- l'émission d'avertissements (envoi de signaux d'avertissement par l'intermédiaire de dispositifs émetteurs correspondants, lumineux et/ou sonores),
- la détection des évènements ; à noter qu'on peut distinguer, parmi les évènements, ceux relatifs aux activités du conducteur (excès de vitesse, chevauchement temporel, dernière session incorrectement clôturée, conduite sans carte appropriée, ...) de ceux relatifs à la sécurité du tachygraphe (insertion d'une carte non valide, conflit de carte, insertion d'une carte en cours de conduite, interruption de l'alimentation électrique, erreur sur les données de mouvement, tentative d'atteinte à la sécurité),
- la détection des anomalies (anomalie sur carte, anomalie sur appareil de contrôle),
- la gestion des verrouillages d'entreprise (traitement de données d'entreprises),
- le suivi des activités de contrôle (dont le traitement des données contrôleur),
- lé contrôle de l'interface de déchargement/étalonnage (connecteur et dispositif émetteur-récepteur d'ondes), la commande de déchargement de données vers un dispositif externe de déchargement, le traitement de données d'étalonnage reçues,
- la réalisation d'autotests,
- le contrôle du circuit CSP 20, selon une relation maître/esclave dans laquelle le microprocesseur principal est le maître et le circuit CSP est l'esclave, et la commande d'opérations de sécurité, le traitement des résultats desdites opérations de sécurité.

[0060] Avantageusement et selon l'invention, les opérations de sécurité en vue de l'authentification mutuelle de l'unité et d'une carte tachygraphique mettent en oeuvre, de préférence, des calculs de chiffrement au moyen de clés asymétriques (clés privées et publiques).

[0061] A noter que cette authentification mutuelle est déclenchée par le microprocesseur principal 4 lorsqu'il constate l'insertion d'une carte tachygraphique dans une interface de réception de carte du dispositif lecteur/enregistreur 8 ou d'un dispositif externe distant communiquant avec le microprocesseur principal 4 par l'intermédiaire de l'interface de cartes 16. Le microprocesseur

principal 4 est en effet adapté pour identifier les insertions et retraits de carte en fonction des signaux qu'il reçoit du (des) organe(s) de détection dudit dispositif lecteur/enregistreur : la présence d'une carte 60 en position de lecture/écriture -réception d'un signal de détection- après une période d'absence de carte -pas de signal de détection- traduit l'insertion d'une carte ; l'absence de carte suite à une période de présence de carte traduit le retrait d'une carte.

[0062] Pour une plus grande sécurité, l'authentification mutuelle d'une carte tachygraphique présente dans le dispositif lecteur/enregistreur est également déclenchée de façon périodique (alors qu'aucun retrait de carte n'a été constaté depuis la précédence authentification) par le microprocesseur principal 4 et/ou par la carte tachygraphique.

[0063] Avantageusement et selon l'invention, les opérations de sécurité en vue de l'authentification de données échangées entre l'unité et le capteur de mouvement ou entre l'unité et une carte tachygraphique, mettent en oeuvre de préférence des calculs de chiffrement au moyen de clés de session, c'est-à-dire de clés symétriques (clés secrètes). Ces clés de session communes au circuit CSP 20 de l'unité et au média externe (capteur de mouvement ou carte tachygraphique) sont établies conjointement par les deux éléments dans le cadre des opérations d'authentification mutuelle de ces éléments ou immédiatement après celles-ci. Les clés de session sont stockées dans la mémoire (protégée) du circuit CSP 20.

[0064] A titre d'exemple simplifié et non limitatif, la lecture de données tachygraphiques sur une carte tachygraphique préalablement authentifiée donne lieu aux opérations illustrées à la figure 3, qui permettent de garantir l'intégrité des données lues (ces opérations visent à vérifier que les données reçues par le microprocesseur principal 4 correspondent à celles envoyées par la carte tachygraphique et que ces dernières n'ont donc pas été falsifiées durant la transmission). Le microprocesseur principal 4 prépare la commande de lecture (étape 30) : le code de commande est assorti de données, dites données annexes, nécessaires à son exécution, telles que l'adresse et la longueur des données tachygraphiques à lire (en vue de leur localisation dans la mémoire de la carte tachygraphique). Il transmet (étape 31) les données annexes au circuit CSP 20, avec une commande d'exécution d'une opération de sécurité correspondante, en vue de protéger l'intégrité desdites données. Le circuit CSP 20 calcule (étape 32) une somme de contrôle, dite checksum, des données annexes, chiffre (encrypte) ladite checksum au moyen de sa clé de session et transmet (étape 33) la checksum cryptée au microprocesseur principal 4. Le microprocesseur principal 4 prépare (étape 34) et transmet (étape 35) la totalité de la commande de lecture (code de commande + données annexes + checksum) à la carte tachygraphique 60 (c'est-à-dire à sa puce électronique 61) via le connecteur du dispositif lecteur/enregistreur 8. La carte tachygraphique 60, 61 vérifie l'intégrité des données reçues (étape 36) en déchiffrant la checksum reçue au moyen de sa clé de session, en calculant la checksum des données annexes reçues et en comparant les deux valeurs. Si ces dernières coïncident, la carte tachygraphique 60, 61 transmet (étape 38) les données tachygraphiques demandées, après avoir préalablement calculé et chiffré -au moyen de sa clé de session- leur checksum (étape 37). A réception des données (étape 39), le microprocesseur principal 4 transmet (étape 40) au circuit CSP 20 les données tachygraphiques et la checksum cryptée reçues, ainsi qu'une commande d'exécution d'une opération de sécurité correspondante visant à vérifier l'intégrité des données tachygraphiques reçues. Exécutant cette commande, le circuit CSP 20 calcule la checksum des données tachygraphiques et déchiffre la checksum cryptée qui les accompagne au moyen de sa clé de session et compare les deux valeurs obtenues (étape 41). Si celles-ci coïncident, il renvoie un signal d'accord au microprocesseur principal 4 ; dans le cas contraire, il transmet à ce dernier un signal de désaccord (étape 42). Le microprocesseur principal 4 n'exploite les données tachygraphiques que si le signal reçu est un signal d'accord (étape 43). Si les données tachygraphiques ne sont pas considérées comme étant authentiques (signal de désaccord), le microprocesseur mémorise l'anomalie et émet éventuellement un signal correspondant à l'attention de l'utilisateur (étape 43).

[0065] Les données de mouvement reçues du capteur de mouvement font également l'objet d'opérations de sécurité en vue de leur authentification. En fait, le capteur de mouvement, préalablement authentifié dans le cadre d'une opération d'appariement avec l'unité, émet continuellement des impulsions qu'il transmet à l'unité, chaque impulsion étant émise à l'instant où une distance prédéterminée a été parcourue par le véhicule depuis l'impulsion précédente. Le capteur de mouvement dispose par ailleurs d'un compteur, qu'il incrémente à chaque impulsion émise. De même, le microprocesseur principal de l'unité dispose d'un compteur, qu'il incrémente à chaque impulsion reçue. Périodiquement, le microprocesseur principal déclenche une opération sécurisée de comparaison des compteurs de capteur et d'unité. La lecture du compteur de capteur s'effectue, par exemple, comme précédemment expliqué relativement à la lecture de données tachygraphiques dans une carte tachygraphique : la valeur du compteur de capteur transmise à l'unité est en particulier authentifiée par un attribut de sécurité de type checksum cryptée. Une valeur relative du compteur de capteur et une valeur relative du compteur d'unité (la valeur relative d'un compteur correspondant à la différence de valeur du compteur depuis la dernière opération de comparaison) sont calculées par le microprocesseur principal puis comparées. Cette procédure permet de vérifier l'authenticité et l'intégrité des données (impulsions) transmises par le capteur pendant la période écoulée depuis la dernière opération de comparaison.

[0066] Il va de soi que l'invention peut faire l'objet de nombreuses variantes par rapport aux modes de réali-

sation précédemment décrits et représentés sur les figures.

Revendications

1. Unité de tachygraphe (1) destinée à être embarquée sur un véhicule automobile et à être reliée à au moins un capteur de mouvement du véhicule, laquelle unité comprend au moins une carte (3) à microprocesseur (s), dite carte principale, pour le traitement et le stockage de données, dites données tachygraphiques, comprenant au moins des données, dites données conducteur, relatives à des activités d'un conducteur dudit véhicule, ladite unité de tachygraphe étant adaptée pour effectuer des opérations, dites opérations de sécurité, mettant en oeuvre des algorithmes de chiffrement en vue de l'authentification d'au moins une partie des données tachygraphiques, **caractérisée en ce que** :

   - ladite carte principale (3) comprend au moins un microprocesseur (4), dit microprocesseur principal, pour le traitement des données tachygraphiques,
   - l'unité comprend au moins un circuit (20) physiquement protégé fournisseur de services cryptographiques, dit circuit CSP, distinct du(des) microprocesseur(s) principal(aux), circuit CSP dans lequel sont stockées au moins des données dites données de sécurité secrètes, ce circuit CSP (20) étant adapté pour réaliser au moins une partie des opérations de sécurité lorsque l'unité est embarquée sur un véhicule.

2. Unité selon la revendication 1, **caractérisée en ce que** la carte principale (3) comprend au moins une mémoire (5), dite mémoire d'application, associée à un microprocesseur principal (4), dans laquelle est stockée une application, dite application tachygraphique, pouvant être chargée dans ce microprocesseur principal pour le traitement des données tachygraphiques, et **en ce que** ce microprocesseur principal est adapté pour pouvoir vérifier l'authenticité d'au moins une partie de l'application tachygraphique à l'aide d'au moins une opération de sécurité réalisée par un circuit CSP (20) de l'unité de tachygraphe.

3. Unité selon la revendication 2, **caractérisée en ce que** ce microprocesseur principal (4) intègre un programme de démarrage protégé, physiquement inscrit dans le microprocesseur et adapté pour, lors d'une opération visant à implémenter au moins une partie d'une application tachygraphique dans l'unité, commander audit circuit CSP (20) l'exécution d'au moins une opération de sécurité en vue de l'authentification de ladite application ou partie d'application tachygraphique, et ne commander l'enregistrement de cette application ou partie d'application tachygraphique dans la mémoire d'application (5) que si elle est considérée par le circuit CSP comme étant authentique et intègre.

4. Unité selon l'une des revendications 2 ou 3, **caractérisée en ce que** l'application tachygraphique stockée dans la mémoire d'application (5) est adaptée pour, lorsqu'elle est chargée dans le microprocesseur principal, commander périodiquement au circuit CSP (20) l'exécution d'au moins une opération de sécurité en vue de l'authentification de ladite application tachygraphique.

5. Unité selon l'une des revendications 1 à 4, **caractérisée en ce que** le(s) circuit(s) CSP (20) est(sont) dédié(s) essentiellement à la réalisation d'opérations de sécurité.

6. Unité selon l'une des revendications 1 à 5, **caractérisée en ce que** le(s) circuit(s) CSP (20) est(sont) dédié(s) essentiellement à la réalisation de toutes les opérations de sécurité.

7. Unité selon l'une des revendications 1 à 6, **caractérisée en ce que** chaque circuit CSP (20) est relié à un microprocesseur principal (4), lesdits circuit CSP et microprocesseur principal associés étant adaptés pour fonctionner selon une relation maître/esclave dans laquelle le microprocesseur principal est le maître et le circuit CSP est l'esclave.

8. Unité selon l'une des revendications 1 à 7, **caractérisée en ce que** le(s) circuit(s) CSP (20) est(sont) porté(s) par la carte principale (3).

9. Unité selon l'une des revendications 1 à 8, **caractérisée en ce que** :

   - l'unité comprend un dispositif (8) lecteur/enregistreur de cartes à puce, dites cartes tachygraphiques, apte à recevoir au moins deux cartes tachygraphiques en parallèle, chaque carte appartenant à un type de carte prédéterminé,
   - le dispositif lecteur/enregistreur de cartes (8) est contrôlé par au moins un microprocesseur principal (4) auquel est associé un circuit CSP (20), ledit microprocesseur principal étant adapté pour commander audit circuit CSP l'exécution d'au moins une opération de sécurité en vue de l'authentification mutuelle de l'unité et d'une carte tachygraphique présente dans le dispositif lecteur/enregistreur de cartes, et n'autoriser l'ouverture d'une session de fonctionnement correspondant au type de la carte tachygraphique présente que si l'unité et ladite carte sont considérées comme étant authentiques.

10. Unité selon la revendication 9, **caractérisée en ce que** ce microprocesseur principal (4) est adapté pour surveiller les insertions et retraits de carte dans le dispositif (8) lecteur/enregistreur de cartes, et commander l'exécution de cette(ces) opération(s) de sécurité dès qu'une insertion d'une carte tachygraphique dans le dispositif lecteur/enregistreur de cartes est détectée.

11. Unité selon l'une des revendications 1 à 10, **caractérisée en ce que**:

- l'unité comprend une interface de connexion (16), dite interface de carte, pour une communication sans fil de l'unité avec un dispositif externe lecteur/enregistreur de cartes à puce, dites cartes tachygraphiques, chaque carte appartenant à un type de carte prédéterminé,
- ledit dispositif lecteur/enregistreur externe est contrôlé par au moins un microprocesseur principal (4) auquel est associé un circuit CSP (20), ledit microprocesseur principal étant adapté pour commander audit circuit CSP l'exécution d'au moins une opération de sécurité en vue de l'authentification mutuelle de l'unité et d'une carte tachygraphique présente dans le dispositif lecteur/enregistreur de cartes, et n'autoriser l'ouverture d'une session de fonctionnement correspondant au type de la carte tachygraphique présente que si l'unité et ladite carte sont considérées comme étant authentiques.

12. Unité selon l'une des revendications 9 à 11, **caractérisée en ce que**, à chaque échange de données entre l'unité (1) et une carte tachygraphique (60) présente dans le dispositif lecteur/enregistreur de cartes, ledit microprocesseur principal (4) est adapté pour commander audit circuit CSP (20) l'exécution d'au moins une opération de sécurité en vue de l'authentification desdites données, et ne traiter les données échangées que si elles sont considérées comme étant authentiques et intègres.

13. Unité selon la revendication 12, **caractérisée en ce que** le microprocesseur principal (4) est adapté pour :

- lorsque des données sont reçues par l'unité depuis ladite carte tachygraphique, commander au circuit CSP (20) l'exécution d'au moins une opération de sécurité en vue de l'authentification des données reçues, et ne traiter lesdites données que si elles sont considérées par le circuit CSP comme étant authentiques et intègres,
- lorsque des données doivent être transmises par l'unité à ladite carte tachygraphique, commander au circuit CSP (20) l'exécution d'au moins une opération de sécurité en vue de la protection de l'intégrité des données à transmettre.

14. Unité selon l'une des revendications 1 à 13, comprenant une interface de connexion (12), dite interface de capteur, pour la liaison de l'unité au capteur de mouvement, **caractérisée en ce que** la carte principale (3) comprend au moins un microprocesseur principal (4) relié à ladite interface de capteur (12) et auquel est associé un circuit CSP (20), ledit microprocesseur principal (4) étant adapté pour commander audit circuit CSP (20) l'exécution d'opérations de sécurité en vue d'une part de l'authentification mutuelle du capteur de mouvement et de l'unité et d'autre part de l'authentification des données de mouvement reçues du capteur de mouvement par l'unité, et ne traiter les données de mouvement reçues que si le capteur de mouvement et l'unité sont considérés comme étant authentiques et si les données reçues sont considérées comme étant authentiques et intègres.

15. Unité selon la revendication 14, **caractérisée en ce que** ledit microprocesseur principal (4) est adapté pour :

- dans le cadre d'une opération initiale dite opération d'appariement d'un capteur de mouvement et de l'unité, commander audit circuit CSP (20) l'exécution d'au moins une opération de sécurité en vue de l'authentification mutuelle du capteur et de l'unité, et n'autoriser un échange ultérieur de données entre ledit capteur et l'unité que si ces derniers sont considérés comme étant authentiques,
- dans le cadre d'une opération périodique, dite opération de contrôle des données de mouvement, commander au circuit CSP (20) l'exécution d'au moins une opération de sécurité en vue de l'authentification de données, dites données de contrôle, échangées entre le capteur et l'unité dans le cadre de cette opération de contrôle, et n'autoriser le traitement des données de mouvement reçues par l'unité sur une période écoulée que si lesdites données de contrôle sont considérées comme étant authentiques et intègres.

16. Unité selon les revendications 15 et 9, **caractérisée en ce que** le(s) microprocesseur(s) principal(aux) (4) est(sont) adapté(s) pour n'autoriser l'exécution d'une opération d'appariement que dans le cadre d'une session d'atelier.

17. Unité selon l'une des revendications 1 à 16 et selon l'une des revendications 9 ou 11, **caractérisée en ce que** :

- elle comprend une interface de connexion (13,

14), dite interface de déchargement, pour la communication de l'unité avec un dispositif externe dit dispositif de déchargement, apte à mémoriser des données tachygraphiques,
- le(s) microprocesseur(s) principal(aux) (4) est (sont) adapté(s) pour n'autoriser l'exécution d'une opération de déchargement de données vers un dispositif de déchargement connecté à l'unité par l'intermédiaire de l'interface de déchargement, que dans le cadre d'une session de contrôleur ou d'atelier ou d'entreprise.

18. Unité selon l'une des revendications 1 à 17 et selon la revendication 9, **caractérisée en ce que** :

- elle comprend une interface de connexion (13, 14), dite interface d'étalonnage, pour la communication de l'unité avec un dispositif externe dit dispositif d'étalonnage,
- le(s) microprocesseur(s) principal(aux) (4) est (sont) adapté(s) pour n'autoriser l'exécution d'une opération d'étalonnage de l'unité, au moyen d'un dispositif d'étalonnage connecté à l'unité par l'intermédiaire de l'interface d'étalonnage, que dans le cadre d'une session d'atelier.

19. Unité selon l'une des revendications 1 à 18 et selon la revendication 9, **caractérisée en ce qu'**un microprocesseur principal (4) de l'unité est adapté pour surveiller les insertions et retraits de carte dans le dispositif (8) lecteur/enregistreur de cartes et pour, dès qu'un retrait d'une carte tachygraphique du dispositif lecteur/enregistreur de cartes est détecté, interrompre toute opération en cours dans la session de fonctionnement correspondante.

20. Unité selon l'une des revendications 1 à 19, **caractérisée en ce que** :

- la carte principale (3) comprend un unique microprocesseur principal (4) pour le traitement des données tachygraphiques, auquel sont reliés un circuit d'alimentation électrique (6) alimenté de façon permanente par une source électrique permanente du véhicule, une mémoire de masse (5), dite mémoire d'application, de type non volatile pour le stockage d'au moins une application dite application tachygraphique, une mémoire de masse (17), dite mémoire de données, de type non volatile pour le stockage au moins des données tachygraphiques, une horloge temps réel calendaire (7), un dispositif (8) lecteur/enregistreur de cartes à puce, dites cartes tachygraphiques, apte à recevoir au moins deux cartes tachygraphiques en parallèle, un connecteur (12), dit connecteur de capteur, pour la connexion de l'unité au capteur de mouvement, un connecteur (13), dit connecteur de déchargement/étalonnage, pour la connexion à l'unité d'un dispositif externe d'étalonnage ou d'un dispositif externe de déchargement,
- l'unité comprend un unique circuit CSP (20), dédié à la réalisation de toutes les opérations de sécurité, lesdits microprocesseur principal (4) et circuit CSP (20) étant reliés et adaptés pour fonctionner selon une relation maître/esclave dans laquelle le microprocesseur principal est le maître et le circuit CSP est l'esclave,

l'unité comprend une imprimante (10), un écran d'affichage (9), un dispositif (11) de saisie de données par un utilisateur.

21. Véhicule automobile, **caractérisé en ce qu'**il est équipé d'une unité de tachygraphe selon l'une des revendications 1 à 20.

Claims

1. A speedograph unit (1) intended to be fitted in a motor vehicle and to be connected to at least one vehicle movement sensor, said unit comprising at least one microprocessor card (3), called the main card, for processing and storing data, called tacographic data, comprising at least some data, called conductive data, relating to activities of a conductor of said vehicle, said speedograph unit being adapted to perform operations, called safety operations, using cryptographic algorithms to authenticate at least part of the tacographic data,
characterised in that:

- said main card (3) comprises at least one microprocessor (4), called the main microprocessor, for processing tachographic data,
- the unit comprises at least one physically protected circuit (20) providing cryptographic services, called the CSP circuit, separate from the main microprocessor(s), wherein are stored at least data called secret safety data, this CSP circuit (20) being adapted to perform at least part of the safety operations when the unit is on board a vehicle.

2. The unit according to Claim 1, **characterised in that** the main card (3) comprises at least one memory (5), called the application memory, associated with a main microprocessor (4), wherein is stored an application, called the tachographic application, that can be loaded into this main microprocessor in order to process the tachographic data, and **in that** this main microprocessor is adapted to be able to check the authenticity of at least part of the tachographic application with the aid of at least one safety opera-

tion performed by a CSP circuit (20) of the speedograph unit.

3. The unit according to Claim 2, **characterised in that** this main microprocessor (4) integrates a protected start-up programme, physically entered in the microprocessor and adapted, during an operation seeking to implement at least part of a tachographic application in the unit, to order said CSP unit (20) to execute at least one safety operation to authenticate said tachographic application or part application, and to only order the recording of this tachographic application or part application in the application memory (5) if it is considered by the CSP circuit to be authentic and integral.

4. The unit according to any of Claims 2 or 3, **characterised in that** the tachographic application stored in the application memory (5) is adapted, when it is loaded in the main microprocessor, to periodically order the CSP circuit (20) to perform at least one safety operation to authenticate said tachographic application.

5. The unit according to any of Claims 1 to 4, **characterised in that** the CSP circuit(s) (20) is(are) essentially dedicated to performing safety operations.

6. The unit according to any of Claims 1 to 5, **characterised in that** the CSP circuit(s) (20) is(are) essentially dedicated to performing all of the safety operations.

7. The unit according to any of Claims 1 to 6, **characterised in that** each CSP unit (20) is connected to a main microprocessor (4), said CSP circuit and the associated main microprocessor being adapted to function according to a master/slave relationship wherein the main microprocessor is the master and the CSP circuit is the slave.

8. The unit according to any of Claims 1 to 7, **characterised in that** the CSP circuit(s) (20) is(are) carried by the main card (3).

9. The unit according to any of Claims 1 to 8, **characterised in that**:

- the unit comprises a device (8) for reading/recording chip cards, called tachographic cards, able to receive at least two tachographic cards in parallel, each card belonging to a predetermined type of card,
- the card reading/recording device (8) is controlled by at least one main microprocessor (4) with which is associated a CSP circuit (20), said main microprocessor being adapted to order said CSP circuit to perform at least one safety operation to authenticate mutually the unit and a tachographic card present in the card reading/recording device and to only authorise the opening of a functioning session corresponding to the type of tachographic card present if the unit and said card are considered to be authentic.

10. The unit according to Claim 9, **characterised in that** this main microprocessor (4) is adapted to monitor the card insertions into and withdrawals from the card reading/recording device (8) and to order the performance of this(these) safety operation(s) as soon as the insertion of a tachographic card into the card reading/recording device is detected.

11. The unit according to any of Claims 1 to 10, **characterised in that**:

- the unit comprises a connection interface (16), called the card interface, for wireless communication of the unit with an external device for reading/recording chip cards, called tachographic cards, each card belonging to a predetermined card type,
- said external reading/recording device is controlled by at least one main microprocessor (4) with which is associated a CSP circuit (20), said main microprocessor being adapted to order said CSP circuit to perform at least one safety operation to mutually authenticate the unit and a tachographic card present in the card reading/recording device, and to only authorise the opening of a functioning session corresponding to the type of tachographic card present if the unit and said card are considered to be authentic.

12. The unit according to any of Claims 9 to 11, **characterised in that** upon each exchange of data between the unit (1) and a tachographic card (60) present in the card reading/recording device, said main microprocessor (4) is adapted to order said CSP circuit (20) to perform at least one safety operation to authenticate said data, and to only process the data exchanged if they are considered to be authentic and integral.

13. The unit according to Claim 12, **characterised in that** the main microprocessor (4) is adapted :

- when data are received by the unit from said tachographic card, to order the CSP circuit (20) to perform at least one safety operation to authenticate the received data and to only process said data if they are considered by the CSP circuit to be authentic and integral,
- when data have to be transmitted by the unit to said tachographic card, to order the CSP cir-

cuit (20) to perform at least one safety operation to protect the integrity of the data to be transmitted.

14. The unit according to any of Claims 1 to 13, comprising a connection interface (12), called the sensor interface, for connecting the unit to the movement sensor, **characterised in that** the main card (3) comprises at least one main microprocessor (4) connected to said sensor interface (12) and with which is associated a CSP circuit (20), said main microprocessor (4) being adapted to order said CSP circuit (20) to perform safety operations on the one hand to mutually authenticate the movement sensor and the unit, and on the other hand to authenticate movement data received from the movement sensor by the unit, and to only process the movement data received if the movement sensor and the unit are considered to be authentic and if the data received are considered to be authentic and integral.

15. The unit according to Claim 14, **characterised in that** said main microprocessor (4) is adapted:

- within the framework of an initial operation called the movement sensor and the unit matching operation, to order said CSP circuit (20) to perform at least one safety operation to authenticate mutually the sensor and the unit, and to only authorise a subsequent exchange of data between said sensor and the unit if the latter are considered to be authentic,
- within the framework of a periodic operation, called the movement data control operation, to order the CSP circuit (20) to perform at least one safety operation to authenticate data, called control data, exchanged between the sensor and the unit within the framework of this control operation, and to only authorise the processing of the movement data received by the unit over a period that has passed if said control data are considered to be authentic and integral.

16. The unit according to Claims 15 and 9, **characterised in that** the main microprocessor(s) (4) is(are) adapted to only authorise the performance of a matching operation within the framework of a workshop session.

17. The unit according to any of Claims 1 to 16 and according to any of Claims 9 to 11, **characterised in that**:

- it comprises a connection interface (13, 14), called the unloading interface, for communication of the unit with an external device called the unloading device, able to memorise tachographic data,
- the main microprocessor(s) (4) is(are) adapted to only authorise the performance of a data unloading operation to an unloading device connected to the unit by means of the unloading interface within the framework of a controller or workshop or business session.

18. The unit according to any of Claims 1 to 17 and according to Claim 9, **characterised in that**:

- it comprises a connection interface (13, 14), called the calibration interface, for communication of the unit with an external device called the calibration device,
- the main microprocessor(s) (4) is(are) adapted to only authorise the performance of a calibration operation of the unit by means of a calibration device connected to the unit by means of the calibration interface within the framework of a workshop session.

19. The unit according to any of Claims 1 to 18 and according to Claim 9, **characterised in that** a main microprocessor (4) of the unit is adapted to monitor the card insertions into and withdrawals from the card reading/recording device (8) and, as soon as a tachographic card withdrawal from the card reading/recording device is detected, to interrupt any ongoing operation in the corresponding functioning session.

20. The unit according to any of Claims 1 to 19, **characterised in that**:

- the main card (3) comprises a single main microprocessor (4) for processing tachographic data to which are connected an electrical supply circuit (6) supplied permanently by a permanent electrical source of the vehicle, a mass memory (5), called the application memory, of the non-volatile type, for storing at least one application called the tachographic application, a mass memory (17), called the data memory, of the non-volatile type for storing at least tachographic data, a real time calendar clock (7), a device (8) for reading/recording chip cards, called tachographic cards, able to receive at least two tachographic cards in parallel, a connector (12), called the sensor connector, for connecting the unit to the movement sensor, a connector (13), called the unloading/calibration connector, for connecting to the unit an external calibration device or an external unloading device,
- the unit comprises a single CSP circuit (20) dedicated to performing all of the safety operations, said main microprocessor (4) and CSP circuit (20) being connected and able to function according to a master/slave relationship wherein the main microprocessor is the master and

the CSP circuit is the slave,
- the unit comprises a printer (10), a display screen (9), a device (11) for data input by a user.

21. A motor vehicle, **characterised in that** it is equipped with a speedograph unit according to any of Claims 1 to 20.

Patentansprüche

1. Tachograph (1) zur Mitnahme in einem Kraftfahrzeug, der an mindestens einen Bewegungssensor des Fahrzeugs angeschlossen wird und mindestens eine Mikroprozessor(en)karte (3), Hauptkarte genannt, enthält, zur Verarbeitung und Speicherung von Daten, Tachographendaten genannt, wobei besagte Tachographendaten mindestens Daten über die Aktivitäten eines Fahrers besagten Fahrzeugs, Fahrerdaten genannt, enthalten und besagter Tachograph geeignet ist, sogenannte Sicherheitsoperationen auszuführen, bei denen Chiffrieralgorithmen zum Einsatz kommen, um zumindest einen Teil der Tachographendaten zu authentifizieren, **dadurch gekennzeichnet, dass**

- besagte Hauptkarte (3) mindestens einen Mikroprozessor (4), Hauptmikroprozessor genannt, zur Verarbeitung der Tachographendaten enthält,
- der Tachograph mindestens einen physisch geschützten Schaltkreis (20), CSP-Schaltkreis genannt, enthält, der kryptographische Funktionen erfüllt und sich vom (von den) Hauptmikroprozessor(en) unterscheidet und in dem mindestens die sogenannten geheimen Sicherheitsdaten gespeichert sind, wobei dieser CSP-Schaltkreis (20) geeignet ist, zumindest einen Teil der Sicherheitsoperationen auszuführen, wenn sich der Tachograph in einem Fahrzeug befindet.

2. Tachograph nach Anspruch 1, **dadurch gekennzeichnet, dass** die Hauptkarte (3) zumindest einen Speicher (5) besitzt, der Applikationsspeicher genannt wird, einem Hauptmikroprozessor (4) zugeordnet ist, und in dem eine Applikation, Tachographenapplikation genannt, gespeichert ist, die in diesen Hauptmikroprozessor zur Verarbeitung der Tachographendaten geladen werden kann, und dass dieser Hauptmikroprozessor geeignet ist, die Authentizität zumindest eines Teils der Tachographenapplikation mit Hilfe mindestens einer mit dem CSP-Schaltkreis (20) des Tachographen durchgeführten Sicherheitsoperation zu überprüfen.

3. Tachograph nach Anspruch 2, **dadurch gekennzeichnet, dass** in diesen Hauptmikroprozessor (4) ein geschütztes Startprogramm integriert ist, das physisch in den Mikroprozessor eingeschrieben und geeignet ist, bei einer Operation, die darauf abzielt, zumindest einen Teil einer Tachographenapplikation in den Tachographen zu implementieren, besagtem CSP-Schaltkreis (20) den Befehl zur Ausführung mindestens einer Sicherheitsoperation zu geben, im Hinblick auf die Authentifizierung besagter Tachographenapplikation oder eines Teils dieser Applikation, und den Befehl zur Aufzeichnung dieser Tachographenapplikation oder eines Teils davon im Applikationsspeicher (5) erst dann zu geben, wenn sie vom CSP-Schaltkreis als authentisch und sicher eingestuft wurde.

4. Tachograph nach einem der Ansprüche 2 oder 3, **dadurch gekennzeichnet, dass** die im Applikationsspeicher (5) gespeicherte Tachographenapplikation geeignet ist, wenn sie in den Hauptmikroprozessor geladen wurde, dem CSP-Schaltkreis (20) periodische Befehle zur Ausführung mindestens einer Sicherheitsoperation im Hinblick auf die Authentifizierung besagter Tachographenapplikation zu geben.

5. Tachograph nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet, dass** der (die) CSP-Schaltkreis(e) (20) im Wesentlichen der Ausführung von Sicherheitsoperationen dienen.

6. Tachograph nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet, dass** der (die) CSP-Schaltkreis(e) (20) im Wesentlichen der Ausführung aller Sicherheitsoperationen dienen.

7. Tachograph nach einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet, dass** jeder CSP-Schaltkreis (20) mit einem Hauptmikroprozessor (4) verbunden ist, wobei besagter CSP-Schaltkreis und der diesem zugeordnete Hauptmikroprozessor geeignet sind, nach einer Master-Slave-Beziehung zu arbeiten, bei der der Hauptmikroprozessor der "Master" und der CSP-Schaltkreis der "Sklave" ist.

8. Tachograph nach einem der Ansprüche 1 bis 7, **dadurch gekennzeichnet, dass** sich der (die) CSP-Schaltkreis(e) (20) auf der Hauptkarte (3) befindet (befinden).

9. Tachograph nach einem der Ansprüche 1 bis 8, **dadurch gekennzeichnet, dass**

- der Tachograph ein Chipkartenlese-/registriergerät (8) beinhaltet, das geeignet ist, mindestens zwei Chipkarten, Tachographenkarten genannt, nebeneinander aufzunehmen, wobei jede Karte einem vorbestimmten Kartentyp entspricht,

- das Kartenlese-/registriergerät (8) von mindestens einem Hauptmikroprozessor (4) gesteuert wird, dem ein CSP-Schaltkreis (20) zugeordnet ist, wobei besagter Hauptmikroprozessor geeignet ist, besagtem CSP-Schaltkreis den Befehl zur Ausführung mindestens einer Sicherheitsoperation zu geben, im Hinblick auf eine gegenseitige Authentifizierung des Tachographen und einer im Kartenlese-/registriergerät befindlichen Tachographenkarte, und erst dann eine der Art der vorliegenden Tachographenkarte entsprechende Betriebsphase zuzulassen, wenn Tachograph und besagte Karte als authentisch gelten.

10. Tachograph nach Anspruch 9, **dadurch gekennzeichnet, dass** der Hauptmikroprozessor (4) geeignet ist, das Einführen von Karten in das bzw. das Herausnehmen von Karten aus dem Kartenlese-/registriergerät (8) zu überwachen und den Befehl zur Ausführung dieser Sicherheitsoperation(en) zu geben, sobald festgestellt wird, dass eine Tachographenkarte in das Kartenlese-/registriergerät eingeschoben wurde.

11. Tachograph nach einem der Ansprüche 1 bis 10, **dadurch gekennzeichnet, dass**

- der Tachograph eine Verbindungsschnittstelle (16), Kartenschnittstelle genannt, für die drahtlose Verbindung des Tachographen mit einem externen Chipkartenlese-/registriergerät beinhaltet, wobei diese Chipkarten Tachographenkarten genannt werden, und jede Karte einem vorbestimmten Kartentyp entspricht,
- besagtes externes Lese-/registriergerät von mindestens einem Hauptmikroprozessor (4) gesteuert wird, dem ein CSP-Schaltkreis (20) zugeordnet ist, wobei besagter Hauptmikroprozessor geeignet ist, besagtem CSP-Schaltkreis den Befehl zur Ausführung mindestens einer Sicherheitsoperation zu geben, im Hinblick auf eine gegenseitige Authentifizierung des Tachographen und einer im Kartenlese-/registriergerät befindlichen Tachographenkarte, und erst dann eine der Art der vorliegenden Tachographenkarte entsprechende Betriebsphase zuzulassen, wenn Tachograph und besagte Karte als authentisch gelten.

12. Tachograph nach einem der Ansprüche 9 bis 11, **dadurch gekennzeichnet, dass** bei jedem Datenaustausch zwischen dem Tachographen (1) und einer im Kartenlese-/registriergerät befindlichen Tachographenkarte (60) besagter Hauptmikroprozessor (4) geeignet ist, besagtem CSP-Schaltkreis (20) den Befehl zur Ausführung mindestens einer Sicherheitsoperation zu geben, im Hinblick auf die Authentifizierung besagter Daten, und die ausgetauschten Daten erst dann zu verarbeiten, wenn sie als authentisch und sicher gelten.

13. Tachograph nach Anspruch 12, **dadurch gekennzeichnet, dass** der Hauptmikroprozessor (4) geeignet ist,

- wenn der Tachograph Daten von besagter Tachographenkarte erhält, dem CSP-Schaltkreis (20) den Befehl zur Ausführung mindestens einer Sicherheitsoperation zu geben, im Hinblick auf die Authentifizierung der erhaltenen Daten, und besagte Daten erst dann zu verarbeiten, wenn sie vom CSP-Schaltkreis als authentisch und sicher eingestuft wurden,
- wenn Daten vom Tachographen an besagte Tachographenkarte übertragen werden müssen, dem CSP-Schaltkreis (20) den Befehl zur Ausführung mindestens einer Sicherheitsoperation zu geben, im Hinblick auf den Schutz der Integrität der zu übertragenden Daten.

14. Tachograph nach einem der Ansprüche 1 bis 13, beinhaltend eine Verbindungsschnittstelle (12), Sensorschnittstelle genannt, zur Verbindung des Tachographen mit dem Bewegungssensor, **dadurch gekennzeichnet, dass** die Hauptkarte (3) mindestens einen Hauptmikroprozessor (4) enthält, der mit besagter Sensorschnittstelle (12) verbunden ist, und dem ein CSP-Schaltkreis (20) zugeordnet ist, wobei besagter Hauptmikroprozessor (4) geeignet ist, besagtem CSP-Schaltkreis (20) dem Befehl zur Ausführung von Sicherheitsoperationen zu geben, im Hinblick einerseits auf die gegenseitige Authentifizierung des Bewegungssensors und des Tachographen, und andererseits auf die Authentifizierung der vom Bewegungssensor an den Tachographen gelieferten Bewegungsdaten, und die erhaltenen Bewegungsdaten erst dann zu verarbeiten, wenn Bewegungssensor und Tachograph als authentisch und die erhaltenen Daten als authentisch und sicher gelten.

15. Tachograph nach Anspruch 14, **dadurch gekennzeichnet, dass** besagter Hauptmikroprozessor (4) geeignet ist,

- im Rahmen einer ersten Inbetriebnahme, "Paarung" eines Bewegungssensors mit dem Tachographen genannt, besagtem CSP-Schaltkreis (20) den Befehl zur Ausführung mindestens einer Sicherheitsoperation zu geben, im Hinblick auf die gegenseitige Authentifizierung des Sensors und des Tachographen, und einen späteren Datenaustausch zwischen besagtem Sensor und dem Tachographen erst dann zuzulassen, wenn letztere als authentisch gelten,

- im Rahmen eines periodischen Betriebs, Prüfung der Bewegungsdaten genannt, dem CSP-Schaltkreis (20) den Befehl zur Ausführung mindestens einer Sicherheitsoperation im Hinblick auf die Authentifizierung der Daten, Prüfdaten genannt, zu geben, die zwischen dem Sensor und dem Tachographen im Rahmen dieser Prüfung ausgetauscht werden, und die Verarbeitung der vom Tachographen über einen abgelaufenen Zeitraum empfangenen Bewegungsdaten erst dann zuzulassen, wenn besagte Prüfdaten als authentisch und sicher gelten.

16. Tachograph nach Anspruch 15 und 9, **dadurch gekennzeichnet, dass** der (die) Hauptmikroprozessor (en) (4) geeignet ist (sind), die Ausführung einer "Paarung" genannten Operation nur im Rahmen eines Werkstattbesuchs zuzulassen.

17. Tachograph nach einem der Ansprüche 1 bis 16 und nach einem der Ansprüche 9 oder 11, **dadurch gekennzeichnet, dass**

- er eine Verbindungsschnittstelle (13, 14), Entladeschnittstelle genannt, beinhaltet, zur Verbindung des Tachographen mit einer externen Vorrichtung, Entladevorrichtung genannt, die geeignet ist, Tachographendaten zu speichern,
- der (die) Hauptmikroprozessor(en) (4) geeignet ist (sind), das Entladen von Daten in eine mit dem Tachographen über die Entladeschnittstelle verbundene Entladevorrichtung nur im Rahmen eines Besuchs des Prüfers, der Werkstatt oder der Firma zuzulassen.

18. Tachograph nach einem der Ansprüche 1 bis 17 und nach Anspruch 9, **dadurch gekennzeichnet, dass**

- er eine Verbindungsschnittstelle (13, 14), Kalibrierschnittstelle genannt, zur Verbindung des Tachographen mit einer externen Vorrichtung, Kalibriervorrichtung genannt, beinhaltet,
- der (die) Hauptmikroprozessor(en) (4) geeignet ist (sind), das Kalibrieren des Tachographen mittels einer mit dem Tachographen über die Kalibrierschnittstelle verbundenen Kalibriervorrichtung nur im Rahmen eines Werkstattbesuchs zuzulassen.

19. Tachograph nach einem der Ansprüche 1 bis 18, und nach Anspruch 9, **dadurch gekennzeichnet, dass** ein Hauptmikroprozessor (4) des Tachographen geeignet ist, das Einführen von Karten in das bzw. das Herausnehmen von Karten aus dem Kartenlese-/registriergerät (8) zu überwachen, und, sobald die Herausnahme einer Tachographenkarte aus dem Kartenlese-/registriergerät festgestellt wird, jede laufende Operation während der entsprechenden Betriebsphase zu unterbrechen.

20. Tachograph nach einem der Ansprüche 1 bis 19, **dadurch gekennzeichnet, dass**

- die Hauptkarte (3) einen einzigen Hauptmikroprozessor (4) zur Verarbeitung der Tachographendaten beinhaltet, dem ein Speisestromkreis (6) zugeordnet ist, der permanent von einer permanenten Stromquelle des Fahrzeugs gespeist wird, sowie ein nichtflüchtiger Massenspeicher (5), Applikationsspeicher genannt, zur Speicherung mindestens einer Applikation, Tachographenapplikation genannt, ein nichtflüchtiger Massenspeicher (17), Datenspeicher genannt, zur Speicherung mindestens der Tachographendaten, eine Echtzeituhr mit Kalender (7), ein Chipkartenlese-/registriergerät (8), wobei diese Chipkarten Tachographenkarten genannt werden, und das Gerät geeignet ist, mindestens zwei Tachographenkarten nebeneinander aufzunehmen, einen Verbinder (12), Sensorverbinder genannt, um den Tachographen an den Bewegungssensor anzuschließen, einen Verbinder (13), Entlade-/Kalibrierverbinder genannt, um an den Tachographen ein externes Kalibriergerät oder ein externes Entladegerät anzuschließen,
- der Tachograph einen einzigen CSP-Schaltkreis (20) beinhaltet, der zur Durchführung aller Sicherheitsoperationen dient, wobei besagter Hauptmikroprozessor (4) und der CSP-Schaltkreis (20) verbunden und geeignet sind, nach einer Master-Slave-Beziehung zu arbeiten, bei der der Hauptmikroprozessor der "Master" und der CSP-Schaltkreis der "Sklave" ist,
- der Tachograph einen Drucker (10), einen Bildschirm (9) und eine Vorrichtung (11) zur Datenerfassung durch einen Nutzer beinhaltet.

21. Kraftfahrzeug, **dadurch gekennzeichnet, dass** es mit einem Tachographen nach einem der Ansprüche 1 bis 20 ausgestattet ist.

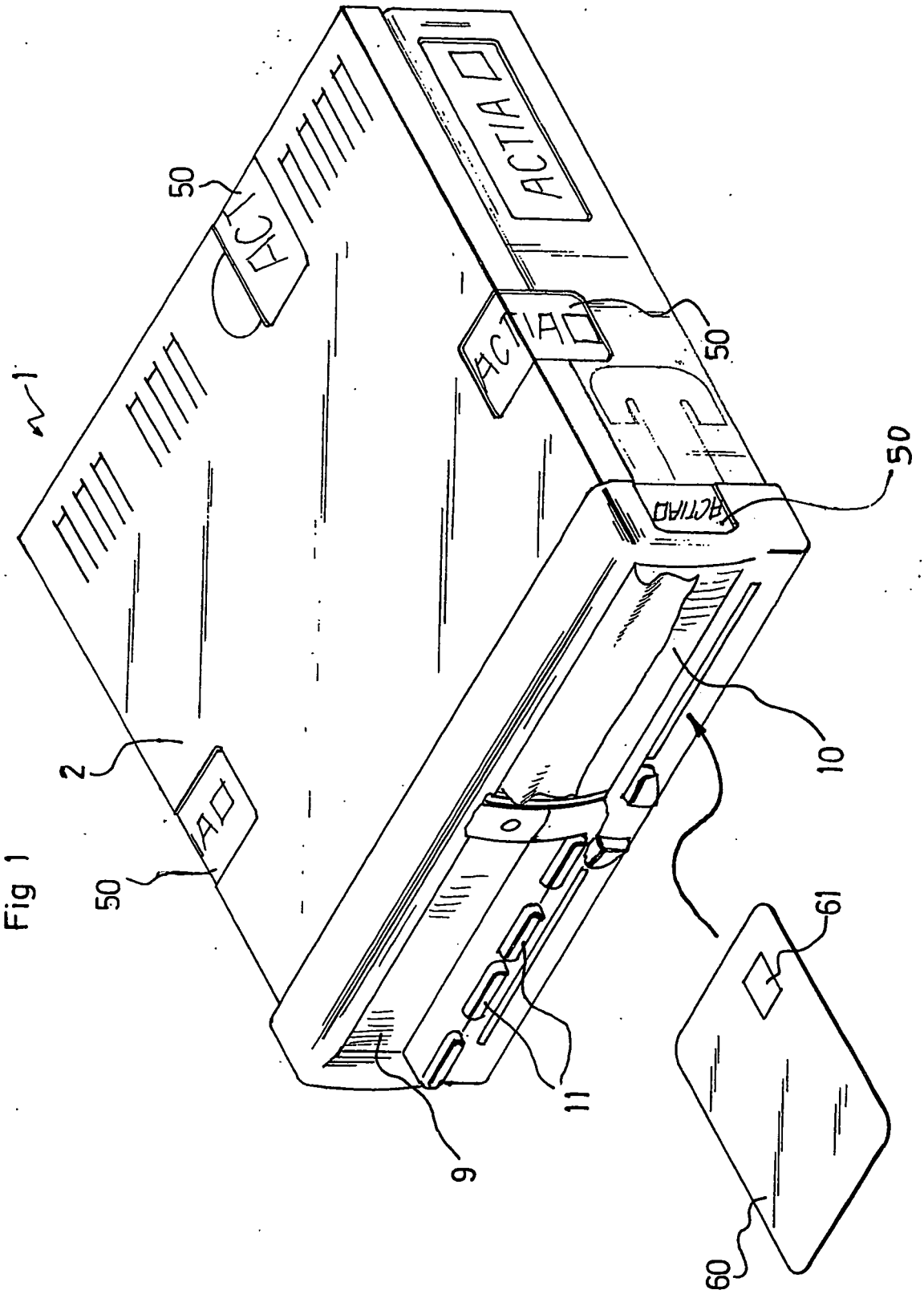


Fig 1

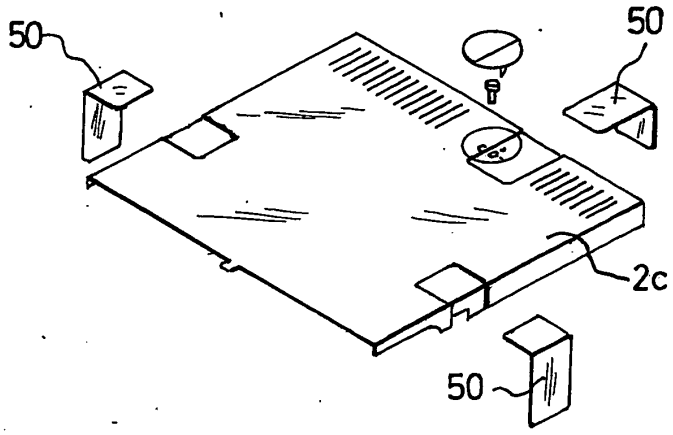
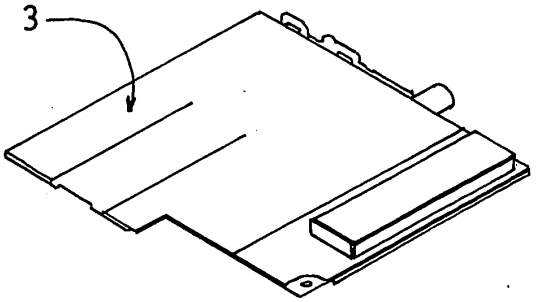
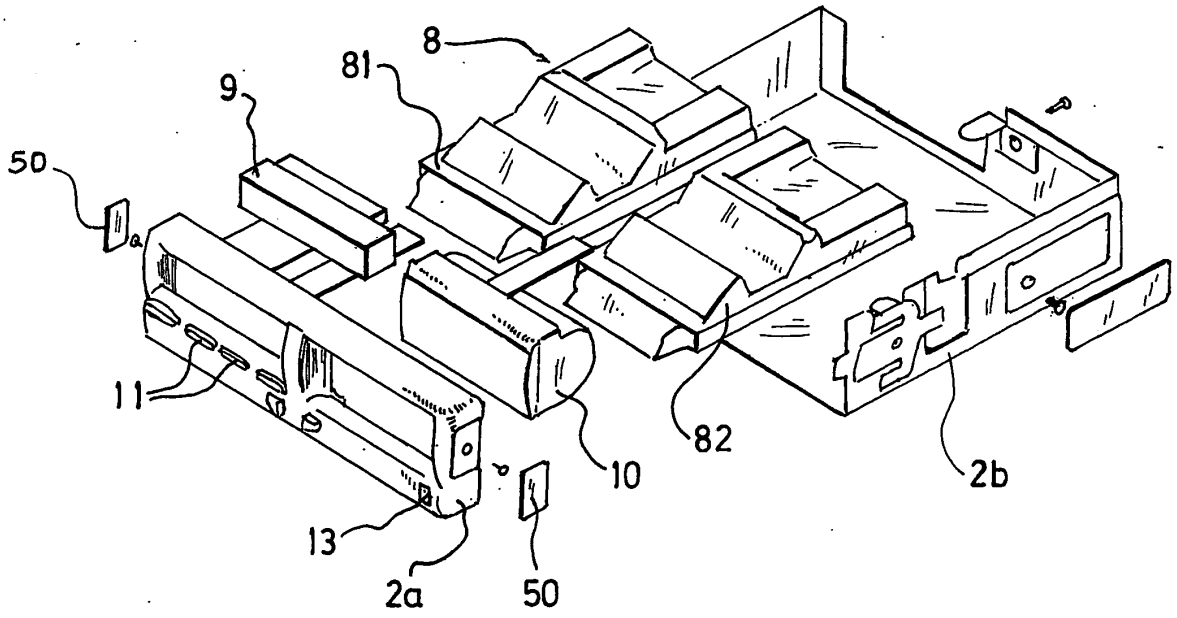


Fig 2





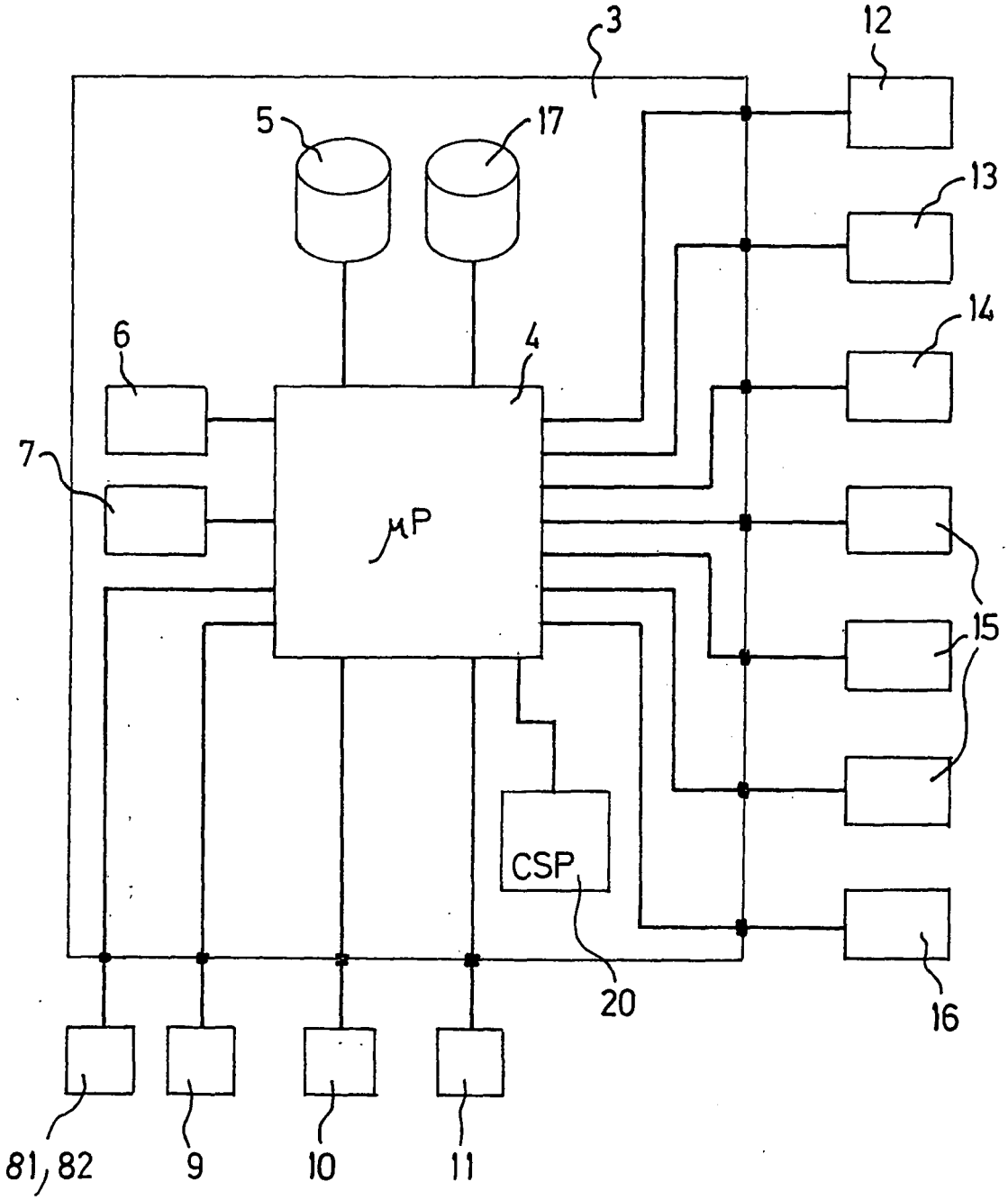
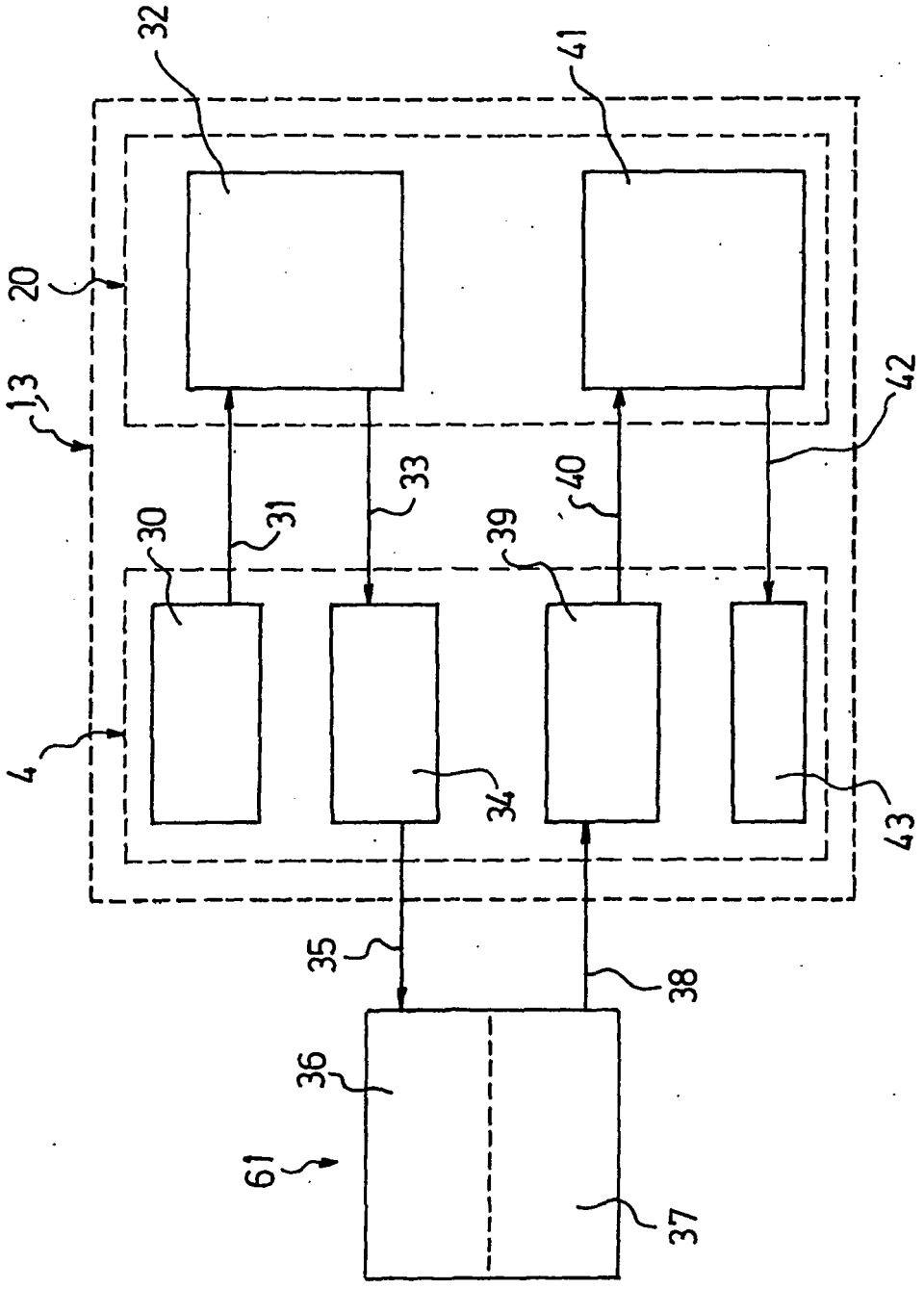


Fig 3

Fig 4



RÉFÉRENCES CITÉES DANS LA DESCRIPTION

Cette liste de références citées par le demandeur vise uniquement à aider le lecteur et ne fait pas partie du document de brevet européen. Même si le plus grand soin a été accordé à sa conception, des erreurs ou des omissions ne peuvent être exclues et l'OEB décline toute responsabilité à cet égard.

Documents brevets cités dans la description

- US 4782691 A **[0003]**
- US 4644368 A **[0004]**
- EP 0592166 A **[0005]**
- WO 0231709 A **[0005]**