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

(11) **EP 2 431 947 A1**

(12) **DEMANDE DE BREVET EUROPEEN**

(43) Date de publication:
21.03.2012 Bulletin 2012/12

(51) Int Cl.:
G07C 5/08 *(2006.01)*

(21) Numéro de dépôt: **10305958.0**

(22) Date de dépôt: **06.09.2010**

(84) Etats contractants désignés:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK SM TR
Etats d'extension désignés:
BA ME RS

(71) Demandeur: **Gemalto SA**
92190 Meudon (FR)

(72) Inventeurs:
- **Rouchouze, Bruno**
  83270, St Cyr sur Mer (FR)
- **Faher, Mourad**
  78160, Marly le Roi (FR)
- **Seif, Jacques**
  75020, Paris (FR)

(54) **Procédé de sécurisation des systèmes électroniques de tachygraphes**

(57) La présente invention propose une solution liant un document officiel électronique normalisé, par exemple le permis de conduire, et la carte conducteur, par un mécanisme cryptographique fort.

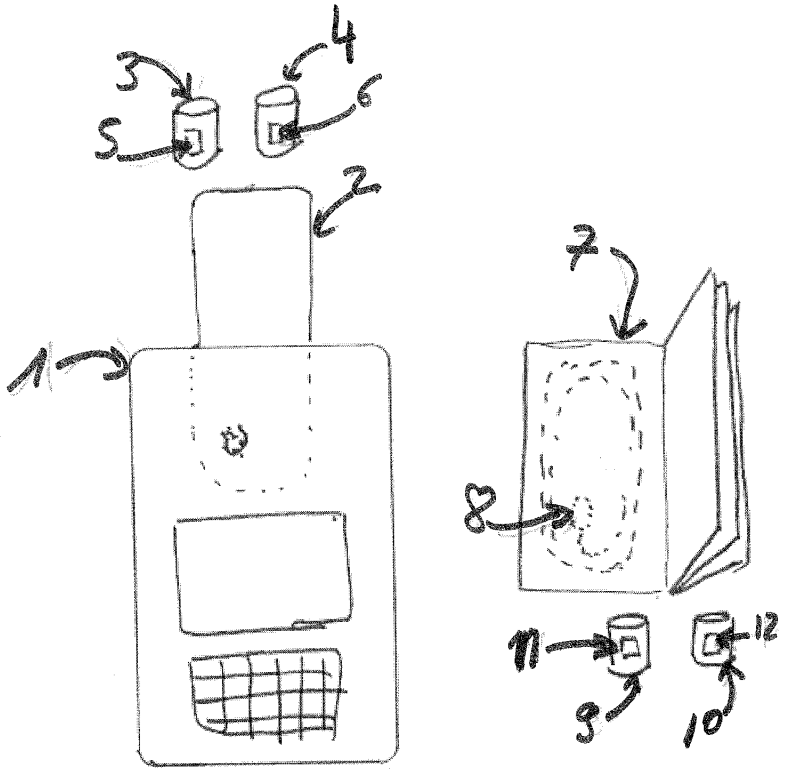

Figure 1

EP 2 431 947 A1

Description

[0001] L'invention concerne un système de sécurisation des systèmes électroniques de tachygraphes.

[0002] L'invention porte en particulier sur une association numérique étroite entre un dispositif électronique de tachygraphe, ainsi qu'un document électronique étatique.

[0003] Le chronotachygraphe, plus généralement appelé tachygraphe, est un appareil électronique enregistreur de vitesse, de temps de conduite et d'activités (travail, attentes...) installé dans un véhicule de transport routier.

[0004] Dans sa version digitale utilisant des disques papiers, la vitesse instantanée du véhicule est enregistrée en regard de l'heure courante. Par une lecture facile, il permet aux conducteurs et aux exploitants de connaître la vitesse suivie, les temps d'arrêt (coupures réglementaires), les temps de conduite ainsi que tous les temps de travail ou de disponibilité, dont le total donnera le temps de service. Il permet de veiller au respect des temps de repos quotidiens et hebdomadaires prescrits par les textes législatifs ainsi qu'au respect des temps de conduite maximaux.

[0005] Les premiers tachygraphes ont été ferroviaires avant même 1900. Comme par exemple le Flaman, ils mettaient en évidence la régularité de la conduite et le respect de la signalisation plus que le temps de conduite.

[0006] Le chronotachygraphe (appelé communément "mouchard") appliqué aux camions existe depuis le début des années 1920. L'enregistrement se fait sur des disques de papier (tachygraphe analogique) ou dans la puce de la carte conducteur (tachygraphe numérique). Le disque (ou la carte) est attaché à chaque conducteur et c'est le temps de service personnel sur la journée qui doit être contrôlé. Il est obligatoire en France, sur tous les véhicules de transports de marchandises (de plus de 3,5 t) et de voyageurs depuis 1969.

[0007] Aujourd'hui le contrôle ne porte plus seulement sur la semaine en cours mais sur les 28 jours précédents; temps de conduite, de travail, de repos journaliers et hebdomadaires seront vérifiés.

[0008] l'installation d'un chronotachygraphe numérique est obligatoire sur les véhicules neufs ainsi qu'en remplacement d'un chronotachygraphe analogique en panne par un UEV (Unité Embarquée du Véhicule) numérique sur les véhicules de transport de personnes de plus de 8 places et sur les véhicules de transport de marchandises de plus de 3,5 tonnes.

[0009] En imposant ce système et une règlementation européenne, l'Union européenne veut améliorer et faciliter le contrôle des temps de conduite et de repos, et combattre ainsi l'une des causes majeures des accidents de la route au niveau des poids lourds. C'est ainsi que la règlementation impose un contrôle de ces appareils tous les 2 ans par des sociétés ayant reçu un agrément de l'état.

[0010] Le système est basé sur un appareil enregistreur scellé et installé par un personnel agréé et assermenté. Il doit comporter un système de stockage permanent et inviolable ainsi qu'une imprimante. Les transferts de données se font par cartes à puces interopérables entre fabricants de système et pays.

[0011] Le chronotachygraphe électronique est un boîtier, de la taille d'un autoradio, comprenant deux lecteurs de cartes, un sélecteur d'entrée manuelle, un écran d'affichage et une imprimante.

[0012] Relié de façon sécurisée au capteur de mouvement, le chronotachygraphe électronique enregistre les données relatives à l'utilisation du véhicule pendant une année. Notamment:

- identification du véhicule ;
- données de calibration ;
- identité du conducteur;
- date et heure d'insertion et d'extraction de la carte conducteur ;
- rapport d'activité ;
- statut de conduite ;
- activité du conducteur;
- alarmes et alertes ;
- localisation de début et de fin de journée
- distance parcourue ;
- pannes et anomalies ;
- identité des agents/corps de contrôle, dates de contrôle(s) ;
- identité de l'atelier, date de calibration ;

[0013] Le chronotachygraphe électronique permet par ailleurs l'impression des données d'activités de façon synthétique.

[0014] Plusieurs cartes à puce relèvent les données, notamment la carte conducteur. De couleur blanche, elle enregistre toutes les activités du conducteur pendant au minimum 28 jours. Personnelle, elle est délivrée par l'Etat où le conducteur possède sa résidence normale. Cette carte s'utilise chaque jour d'activité sur tout véhicule équipé d'un chronotachygraphe électronique. Sa durée de validité est fixée à 5 ans. Grâce à l'interopérabilité du système, la carte de conducteur est lisible par tout chronotachygraphe électronique homologué.

[0015] Dans un mode de fonctionnement nominal, une carte conducteur est associée à un seul et unique chauffeur, et de même, un chauffeur ne possède qu'une seule

carte de conducteur.

[0016] Toutefois, des utilisateurs peu scrupuleux essayent de détourner le système, principalement de deux façons :

[0017] Afin de pouvoir dépasser les limitations légales de conduite, notamment en termes de durée, certains utilisateurs déclarent leur carte conducteur volée, et demande son renouvèlement. Ils se trouvent ainsi en possession de au moins deux cartes conducteur. Il devient donc possible, une fois les limites légales atteintes, de changer de carte conducteur, et donc d'entamer un nouvel enregistrement. De même, suite a une série d'infractions, par exemple de vitesse, il est possible a de tels utilisateurs de changer la carte, afin que, en cas de contrôle, ces données ne soient pas présente sur la carte contrôlée.

[0018] De même, certains utilisateurs tentés de partager une carte conducteur, et ainsi faire conduire une personne non habilitée.

[0019] Une solution, consiste en une base de donnée centralisée des cartes conducteurs, ainsi que des identités des personnes à qui elles ont été délivrées.

[0020] Toutefois, la mise en oeuvre de cette solution s'avère très difficile dans un territoire pluri-étatique tel que l'Europe, ou chaque pays peut délivrer des documents officiels aux formats différents, et dont les législations et les techniques en termes de bases de données, sont très disparates.

[0021] La présente invention propose une solution liant un document officiel électronique normalisé, par exemple le permis de conduire, et la carte conducteur, par un mécanisme cryptographique fort.

[0022] Pour ce faire, l'invention décrit un procédé de sécurisation du système de tachygraphe, comportant au moins un premier dispositif mobile électronique dit dispositif conducteur, et un second dispositif mobile électronique dit dispositif citoyen, chacun comportant, dans une mémoire non volatile, un identifiant unique, ainsi qu'un terminal électronique dit tachygraphe, ledit dispositif conducteur étant configuré pour recevoir et mémoriser des informations en provenance dudit tachygraphe. La mise en service de ce dispositif conducteur comporte en outre les étapes de :

- enregistrement, dans une mémoire non volatile du dispositif conducteur, de l'identifiant unique du dispositif citoyen

- enregistrement, dans une mémoire non volatile du dispositif citoyen, de l'identifiant unique du dispositif conducteur

[0023] Les identifiants enregistrés peuvent être chiffrés à l'aide d'un algorithme cryptographique ALGO, et une clef cryptographique K pour donner des identifiants chiffrés. Ainsi il peut exister au moins un troisième dispositif électronique, dit dispositif de contrôle, apte à communiquer avec les premiers et second dispositifs, et possédant les moyens cryptographique pour vérifier que l'identifiant chiffré enregistré dans le premier dispositif électronique est bien identique à l'identifiant du deuxième dispositif électronique, et que l'identifiant chiffré enregistré dans le deuxième dispositif électronique est bien identique à l'identifiant du premier dispositif électronique.

[0024] Selon un mode de réalisation, le premier dispositif électronique peut être une carte à puce.

[0025] Selon un mode de réalisation, le second dispositif électronique peut être par exemple un permis de conduire électronique, une carte d'identité électronique ou bien un passeport électronique.

[0026] D'autres caractéristiques et avantages de l'invention ressortiront clairement de la description qui en est faite ci-après, à titre indicatif et nullement limitatif, en référence au dessin annexé dans lequel :

- La figure 1 représente un tachygraphe, avec dispositif conducteur selon l'invention, ainsi qu'un dispositif citoyen associé.

[0027] Selon l'invention, le dispositif conducteur est un dispositif électronique possédant au moins une mémoire interne non volatile apte a recevoir et enregistrer des informations issues du tachygraphe électronique, ainsi que à enregistrer au moins une information sécurisée. Cette contrainte technique, associée au contexte général d'utilisation d'un tel dispositif impose des conditions générales de sécurité élevées. Ainsi, un tel dispositif selon l'invention peut avantageusement être une carte a puce, ou une clef USB sécurisée.

[0028] Les contraintes de sécurités associées à ce dispositif conducteur doivent permettre d'enregistrer les informations issues du tachygraphe dans des conditions assurant que aucun utilisateur non habilité ne peut les modifier. La consultation est généralement permise.

[0029] Dans le mode d'implémentation illustré dans la figure 1, un tachygraphe 1 reçoit un dispositif conducteur 2, ici illustré par une carte a puce.

[0030] Selon l'invention, ce dispositif conducteur possède au moins deux zones mémoires :

- une zone 3 de mémoire non volatile, contenant au moins un identifiant unique 5, lié audit dispositif conducteur 2

- une zone mémoire 4 contenant une donnée sécurisée 6, dont l'accès est strictement protégé. Cette protection se fait avantageusement par un chiffrement. Ce chiffrement sera développé plus loin dans la présente description.

[0031] A ce dispositif conducteur est associé un dispositif citoyen 7, ici illustré par un passeport électronique. De manière avantageuse, ce dispositif est un permis de conduire muni d'un composant électronique 8. Ce dispositif possède au moins deux zones mémoires :

- une zone 9 de mémoire non volatile, contenant au moins un identifiant unique 11, lié audit dispositif citoyen 7

- une zone mémoire 10 contenant une donnée sécurisée 12, dont l'accès est strictement protégé.

[0032] La création du dispositif conducteur 2 doit se faire auprès d'une administration étatique possédant des habilitations spécifique. En France, de tels lieux peuvent être par exemple les gendarmeries, les préfectures, ...

[0033] Ces administrations ont en leur possession les moyens informatiques pour lire les données dudit dispositif conducteur, ainsi que dudit dispositif citoyen, mais elles possèdent surtout la possibilité d'enregistrer des informations dans ces mêmes dispositifs.

[0034] En effet lors de la création du dispositif 2, le conducteur a qui se dispositif est destiné doit fournir un dispositif citoyen 7.

[0035] L'agent en charge de l'opération connecte ces deux dispositifs sur un terminal, et au travers de celui-ci, il accède ainsi aux identifiants uniques 5 et 11, respectivement stockés dans les zones mémoires 3 et 9.

[0036] En possession de ces informations, l'agent va pouvoir appairer ces deux dispositifs.

[0037] L'appairage peut prendre plusieurs formes selon l'invention.

[0038] Dans un premier mode de réalisation, cet appairage peut se faire par l'inscription, de l'identifiant 5 du dispositif conducteur dans la donnée sécurisée 12 du dispositif citoyen 7, et inversement, de l'inscription de l'identifiant 11 du dispositif citoyen 7 dans la donnée sécurisée 6 du dispositif conducteur 2.

[0039] Un autre mode d'appairage consiste en l'inscription des deux identifiants 5 et 11 dans chacune des données sécurisées 6 et 12.

[0040] Afin d'optimiser la sécurité du système, le procédé selon l'invention comporte avantageusement un chiffrement des données sécurisées, par exemple grâce à un algorithme cryptographique et une clef.

[0041] Ce chiffrement peut se faire avec l'aide de tout moyen de chiffrement connu de l'homme de l'art, notamment par l'utilisation d'un algorithme symétrique ou asymétrique.

[0042] La cryptographie symétrique, ou cryptographie à clé secrète est basée sur la connaissance partagée d'un secret entre deux acteurs.

[0043] Les algorithmes utilisés, tels que par exemple le DES, 3DES, AES, ... s'appuient sur le fait qu'il est presque impossible, connaissant le chiffré d'un message, de retrouver le message clair sans connaître la clé utilisée pour le chiffrement.

[0044] La cryptographie asymétrique, ou cryptographie à clé publique est fondée sur l'existence de fonctions à sens unique.

[0045] Ainsi, la cryptographie à clé publique est un procédé asymétrique utilisant une paire de clés. Ces clés, généralement baptisées « clé publique » et « clé privée », sont construites de telle manière que, ce qui est chiffré avec l'aide d'une de ces clés ne peut être déchiffré que par la seconde.

[0046] On peut noter qu'il est impossible de deviner la clé privée à partir de la clé publique.

[0047] La génération des couples clé publique/clé privée, ne fait pas l'objet de la présente invention. Tous les procédés décrits par l'état de l'art, ou à venir, qui permettent d'obtenir un tel couple de clé s'appliquent à la présente invention.

[0048] Les clés de type « chiffrement de groupe », qui permettent d'associer à une clé publique, plusieurs clés privées, chacune permettant de déchiffrer tout ou partie de ce qui a été chiffré avec la clé publique, s'appliquent parfaitement à la présente invention.

[0049] Dans un mode sécurisé d'implémentation de l'invention, la lecture des données sécurisées nécessite l'application de clefs cryptographiques qui peuvent être embarquées dans un dispositif dit dispositif de contrôle. Un tel dispositif est, par exemple, en possession des forces de l'ordre, habilitées à contrôler la validité des dispositifs conducteur.

[0050] Ainsi, lors d'un control, le dispositif conducteur est connecté à un terminal, le dispositif de contrôle également. Le dispositif de contrôle comporte des moyens pour stocker au moins une clef cryptographique de manière sécurisée.

[0051] Le terminal lit la donnée sécurisée dans le dispositif conducteur, et le déchiffre. Ce déchiffrement peut se faire dans le terminal, au moyen de la clef contenue dans le dispositif de control, ou bien dans le dispositif de contrôle lui même.

[0052] Cette étape permet d'obtenir au moins une information sur le dispositif citoyen auquel le dispositif conducteur est associé.

[0053] L'agent doit alors lire l'identifiant du dispositif citoyen, et vérifier la concordance avec l'information issue du dispositif conducteur.

[0054] Dans le cas ou la donnée sécurisée contient également l'identifiant du dispositif conducteur, la verification va s étendre a cette donnée.

[0055] De manière préférée, la vérification comporte en outre la lecture de la donnée sécurisée présente dans le dispositif citoyen, son déchiffrement, et une verification des données obtenue, de manière comparable à celle décrite ci-dessus.

Revendications

1. Procédé de sécurisation du système de tachygraphe, comportant au moins un premier dispositif mobile électronique dit dispositif conducteur, et un second dispositif mobile électronique dit dispositif citoyen, chacun comportant, dans une mémoire non volatile, un identifiant unique, ainsi qu'un terminal électronique dit tachygraphe, ledit dispositif conducteur étant configuré pour recevoir et mémoriser des

informations en provenance dudit tachygraphe,
caractérisé en ce que,
la mise en service dudit dispositif conducteur comporte en outre les étapes de :

enregistrement, dans une mémoire non volatile dudit dispositif conducteur, de l'identifiant unique dudit dispositif citoyen
enregistrement, dans une mémoire non volatile dudit dispositif citoyen, de l'identifiant unique dudit dispositif conducteur.

2. Procédé de sécurisation du système de tachygraphe selon la revendication 1, **caractérisé en ce que** lesdits identifiants enregistrés sont chiffrés à l'aide d'un algorithme cryptographique ALGO, et une clef cryptographique K pour donner des identifiants chiffrés.

3. procédé de sécurisation du système de tachygraphe selon la revendication 2, **caractérisé en ce que** il existe au moins un troisième dispositif électronique, dit dispositif de contrôle, apte a communiquer avec les premiers et second dispositifs, et possédant les moyens cryptographique pour vérifier que ledit identifiant chiffré enregistré dans ledit premier dispositif électronique soit bien identique audit identifiant dudit deuxième dispositif électronique, et que ledit identifiant chiffré enregistré dans ledit deuxième dispositif électronique soit bien identique audit identifiant dudit premier dispositif électronique.

4. Procédé de sécurisation du système de tachygraphe selon l'une quelconque des revendications précédentes, **caractérisé en ce que** ledit premier dispositif électronique est une carte à puce.

5. Procédé de sécurisation du système de tachygraphe selon l'une quelconque des revendications précédentes, **caractérisé en ce que** ledit second dispositif électronique est un permis de conduire électronique.

6. Procédé de sécurisation du système de tachygraphe selon l'une quelconque des revendications précédentes, **caractérisé en ce que** ledit second dispositif électronique est une carte d'identité électronique.

7. Procédé de sécurisation du système de tachygraphe selon l'une quelconque des revendications précédentes, **caractérisé en ce que** ledit second dispositif électronique est un passeport électronique.

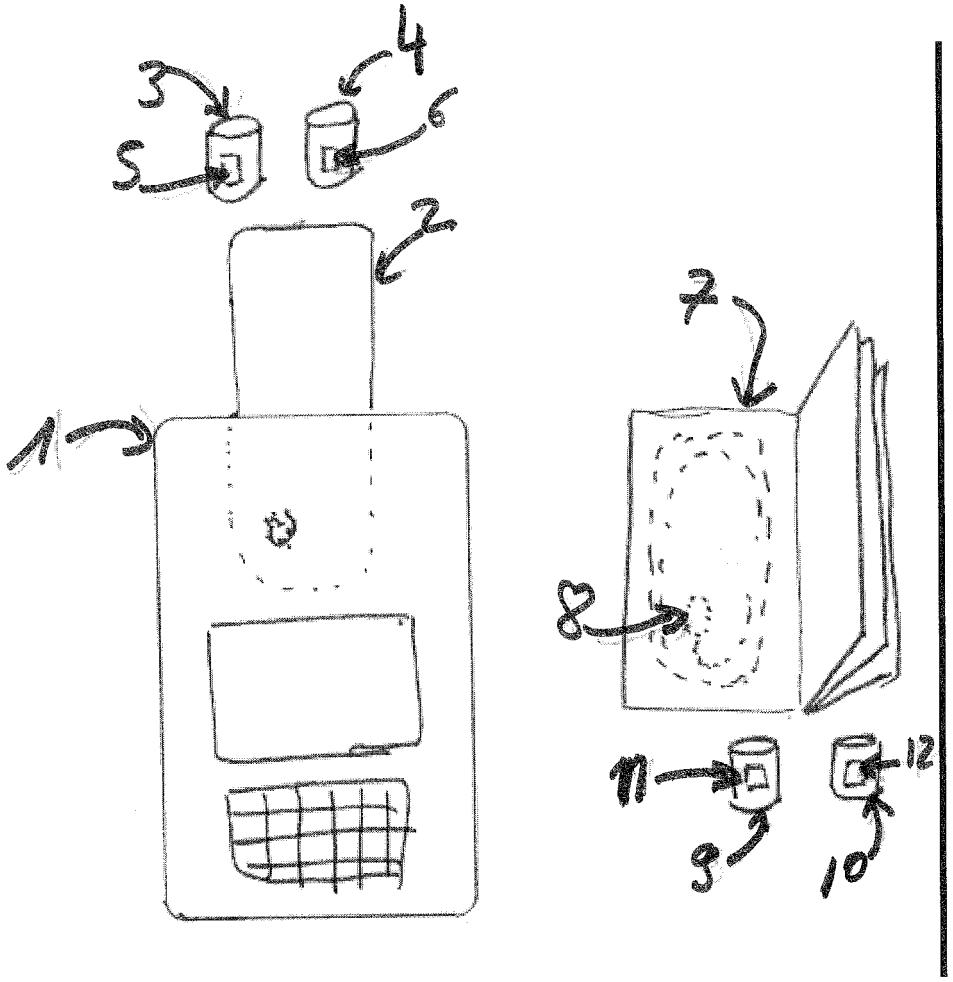

Figure 1

Europäisches Patentamt
European Patent Office
Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 10 30 5958

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (IPC)
Y	DE 10 2007 004645 A1 (SIEMENS AG [DE]) 31 juillet 2008 (2008-07-31) * alinéa [0027] - alinéa [0035] * * figures 1,2 *	1-7	INV. G07C5/08
Y	WO 03/071396 A2 (DIGMARC CORP [US]; CARR J SCOTT [US]; DAVIS BRUCE L [US]; DECKER STEPH) 28 août 2003 (2003-08-28) * page 10, ligne 1 - page 12, ligne 30 *	1-7	
A	EP 2 177 922 A1 (GEMALTO SA [FR]) 21 avril 2010 (2010-04-21) * le document en entier *	1	
A	FR 2 932 914 A1 (GILLES LEROUX IND [FR]) 25 décembre 2009 (2009-12-25) * page 5, ligne 3 - page 7, ligne 32 * * figures *	1	
A	FR 2 916 881 A1 (OBERTHUR CARD SYST SA [FR]) 5 décembre 2008 (2008-12-05) * page 21, ligne 29 - page 24, ligne 19 * * figure 2 *	1	DOMAINES TECHNIQUES RECHERCHES (IPC) G07C

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
Munich	27 janvier 2011	Paraf, Edouard

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons
.....
& : membre de la même famille, document correspondant

1 EPO FORM 1503 03.82 (P04C02)

ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE RELATIF A LA DEMANDE DE BREVET EUROPEEN NO. EP 10 30 5958

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche européenne visé ci-dessus.
Lesdits members sont contenus au fichier informatique de l'Office européen des brevets à la date du
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets.

27-01-2011

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
DE 102007004645 A1	31-07-2008	CN 101589409 A	25-11-2009
		EP 2115703 A1	11-11-2009
		WO 2008090057 A1	31-07-2008
		US 2009327760 A1	31-12-2009
WO 03071396 A2	28-08-2003	AU 2003217642 A1	09-09-2003
		CA 2476895 A1	28-08-2003
		EP 1481347 A2	01-12-2004
EP 2177922 A1	21-04-2010	WO 2010043646 A1	22-04-2010
FR 2932914 A1	25-12-2009	WO 2010007479 A2	21-01-2010
FR 2916881 A1	05-12-2008	EP 2058746 A1	13-05-2009
		US 2008301764 A1	04-12-2008

EPO FORM P0460

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82