BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS

BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE

CHAMBRES DE RECOURS DE L'OFFICE EUROPEEN DES BREVETS

Code de distribution interne :
(A) [ ] Publication au JO
(B) [ ] Aux Présidents et Membres
(C) [ ] Aux Présidents
(D) [x] Pas de distribution

Liste des données pour la décision du 6 mars 2008

N° du recours : T 0984/06 - 3.5.05

N° de la demande : 96400908.8

N° de la publication : 0742656

C.I.B. : H04L 9/32

Langue de la procédure : FR

Titre de l'invention :
Procédé et système pour la sécurisation de la transmission de données entre un capteur et un enregistreur

Demandeur :
ACTIA

Opposant :
-

Référence :
Capteur tachymétrique/ACTIA

Normes juridiques appliquées :
CBE Art. 54, 56, 84, 123(2)
RPCR Art. 12, 13

Normes juridiques appliquées (CBE 1973) :
-

Mot-clé :
Activité inventive (après modification - oui)

Décisions citées :
-

Exergue :
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

N° du recours : T 0984/06 - 3.5.05

D E C I S I O N
de la Chambre de recours technique 3.5.05
du 6 mars 2008

Requérant : ACTIA
Chemin de Pouvourville
F-31400 Toulouse (FR)

Mandataire : Bonnet, Michel
Cabinet JP COLAS
58 rue de Châteaudun
F-75009 Paris (FR)

Décision attaquée : **Décision de la division d'examen de l'Office européen des brevets postée le 9 février 2006 par laquelle la demande de brevet européen n° 96400908.8 a été rejetée conformément aux dispositions de l'article 97(1) CBE.**

Composition de la Chambre :

Président : M-B. Tardo-Dino
Membres : A. Ritzka
M. Höhn

Exposé des faits et conclusions

I. Le présent recours est formé par le demandeur de la demande européenne n° 96400908.8 à l'encontre de la décision rendue le 9 février 2006 par la division d'examen rejetant la demande pour défaut d'activité inventive au vu du document

D2: L. Cooke, "Sensor Technology and Signal Analysis High Security Encryption Supervision", Proceedings of 1990 International Carnahan Conference on Security Technology: Crime Countermesures, Lexington (US), 10 October 1990, pages 29 à 32.

II. Le recours a été déposé le 12 avril 2006. La taxe de recours a été acquittée le même jour. Avec le mémoire de recours, reçu le 30 mai 2006, le requérant a présenté un jeu de revendications principal. Dans le mémoire de recours il a proposé un premier jeu de revendications subsidiaire correspondant au jeu de revendications principal fourni avec le mémoire de recours, dans lequel les revendications 1 et 4 auraient été combinées, et un second jeu de revendications subsidiaire correspondant au jeu de revendications principal fourni avec le mémoire de recours dans lequel les revendications 1 et 6 auraient été combinées. Le requérant a demandé que la Chambre de recours se prononce sur l'activité inventive de l'objet défini dans le jeu de revendications principal, subsidiairement de se prononcer sur l'activité inventive de l'un et/ou de l'autre des objets définis respectivement dans les deux jeux de revendications subsidiaires et, dans l'hypothèse où aucune décision favorable ne serait envisagée, qu'une procédure orale soit organisée.

III. Dans une notification en annexe à une convocation à une procédure orale la Chambre a communiqué ses observations après un examen préliminaire. La revendication 1 selon tous les jeux de revendications ne semblait pas être conforme aux exigences de l'article 123(2) CBE. L'objet de la revendication 1 selon tous les jeux de revendications ne semblait pas impliquer une activité inventive au vu du document D2. En outre, la Chambre a invité le requérant à préciser ses requêtes.

IV. Par courrier du 5 février 2008 le requérant a présenté un troisième jeu subsidiaire de revendications et a précisé en outre sur quels documents les requêtes devaient être basées. Il a annoncé que le représentant de la titulaire serait présent à l'audience.

A la procédure orale, qui a eu lieu le 6 mars 2008, le requérant a présenté une nouvelle requête remplaçant toutes les requêtes précédentes. A la fin de l'audience la décision a été annoncée. La revendication 1 selon la requête principale s'énonce comme suit :

"Procédé pour la sécurisation de la transmission de données entre un capteur (20) délivrant des signaux et un enregistreur (10) traitant ceux-ci, comportant les étapes suivantes :

- établir un échange de données chiffrées entre un module enregistreur (1) comprenant ledit enregistreur et un module capteur (2) comprenant ledit capteur, via une liaison série (3), lesdites données chiffrées comprenant :
  - des messages de commande numériques (M_C) générés et chiffrés par le module enregistreur (1), et

- des messages de retour numériques (M_R) comprenant des messages générés et chiffrés par le module capteur (2) en réponse à des messages de commande reçus et déchiffrés, et

- effectuer un déchiffrement et une vérification des messages de retour reçus par le module enregistreur (1) pour valider en permanence l'intégrité de la liaison et des données,

caractérisé en ce que

- lesdits messages de commande (M_C) sont chiffrés dans ledit module enregistreur (1) et déchiffrés dans ledit module capteur (2) au moyen d'un premier code de chiffrement C,
- lesdits messages de retour (M_R) sont chiffrés dans ledit module capteur (2) et déchiffrés dans ledit module enregistreur (1) au moyen d'un second code de chiffrement C',
- ledit capteur (20) est un capteur tachymétrique qui délivre des impulsions et lesdits messages de retour (MR) comprennent en outre des messages générés par ledit module capteur (2) pour la transmission desdites impulsions en vue de leur restitution pour leur traitement par le module enregistreur,
- et en ce que les messages de commande comprennent des messages de demande de réinitialisation des codes de chiffrement C et C', en ce que les messages de retour correspondants comprennent une information relative à l'acquittement de la réinitialisation, et en ce que l'étape de vérification consiste à contrôler que la réinitialisation demandée a été acquittée."

La revendication 8 porte sur un système adapté à l'exécution du procédé selon la revendication 1.

Motifs de la décision

1. *Recevabilité*

Selon l'article 12 du règlement des procédures des Chambres de recours, la procédure de recours se fonde sur l'acte de recours et le mémoire exposant les motifs du recours déposés ainsi que sur toute notification envoyée par la Chambre et toute réponse à celle-ci produite conformément aux ordonnances de la Chambre. L'admission et l'examen de toute modification présentée par une partie après que celle-ci a déposé son mémoire exposant les motifs du recours ou sa réponse sont laissés à l'appréciation de la Chambre selon l'article 13 RPCR.

La revendication 1 selon la requête qui n'a été présentée qu'à la procédure orale ne diffère de la revendication 1 selon la requête subsidiaire présentée avec le courrier du 5 février 2008 que par la formulation en deux parties et la clarification que les impulsions sont transmises en vue de leur restitution pour leur traitement par le module enregistreur. La Chambre considère que la différence entre la revendication 1 telle que présentée à l'audience et la revendication 1 selon la requête subsidiaire 2 qui a été déposée un mois avant l'audience est d'une complexité modérée de sorte que la chambre peut décider à son sujet sans qu'il soit nécessaire de retarder la procédure; la requête présentée à l'audience est donc recevable.

2. *Articles 84 et 123(2) CBE*

La revendication 1 correspond à une combinaison des revendications 1, 4 et 11, telles que publiées, dans laquelle il est précisé que les messages sont générés par ledit module capteur pour la transmission desdites impulsions en vue de leur restitution pour leur traitement par le module enregistreur. Cette spécification est basée sur la colonne 5, ligne 25 à 28 de la description telle que publiée. Les revendications 2 à 7 correspondent aux revendications 2, 3 et 5 à 8 telles que publiées. La revendication 8 correspond à la revendication 9 telle que publiée, adaptée au procédé selon la revendication 1. L'adaptation se base sur les revendications 9 et 11 telles que publiées et la colonne 4, lignes 22 à 31 de la description telle que publiée.

Les pages 1 à 6 de la description présentées à l'audience correspondent aux pages de la description telle que publiée, adaptée aux revendications de la requête présentée à l'audience et ajoutant la référence au document D2 dans l'introduction de la description. Les dessins 1, 2A, 2B présentés à l'audience correspondent aux dessins tels que publiés à l'exception des corrections à la figure 2A et 2B faites lors de la procédure d'examen et basées sur la colonne 4, lignes 29 à 31 de la description telle que publiée.

Les modifications contenues dans les documents de la requête présentée à l'audience sont conformes aux exigences des articles 84 et 123(2) CBE.

3. *Nouveauté et activité inventive*

3.1 Document de l'art antérieur le plus pertinent

Le document D2 est considéré comme document de l'art antérieur le plus pertinent.

D2 donne un aperçu de la sécurisation des connexions par lesquelles des messages d'un capteur sont transmis à une centrale dans le contexte d'établissements nucléaires ou militaires sensibles. Dans ce contexte des fraudes par des capteurs modifiés ou des données falsifiées par des saboteurs internes posent un problème.

Une possibilité divulguée consiste à utiliser une connexion analogique surveillée par des moyens électriques. Une autre possibilité consiste à utiliser une connexion numérique par laquelle les messages qui sont convertis de l'analogique en numérique sont transmis. Bien que la sécurité d'une connexion numérique soit supérieure à celle d'une connexion analogique, les messages peuvent être falsifiés par des méthodes sophistiquées. C'est la raison pour laquelle la troisième possibilité est préférée qui consiste à utiliser une transmission des messages numériques chiffrés par la connexion numérique. D2 divulgue d'utiliser un module capteur qui est lié à un module d'enregistrement. Le module capteur comprend, outre le capteur, un microprocesseur qui ajoute aux données générées à la base du signal fourni par le capteur des nombres aléatoires et chiffre ce message en utilisant un algorithme de clé. En outre le message chiffré comprend des données d'état, par exemple l'information qu'une porte est ouverte ou fermée, et des messages de commande.

L'algorithme utilisé pour le chiffrement et le déchiffrement peut être différent dans les deux directions pour augmenter la sécurité.

Le problème à la base du document D2 est de protéger la transmission de messages entre un capteur et une centrale dans un établissement sensible contre des falsifications de messages par des saboteurs internes. Ce problème est comparable au problème à la base de la revendication 1 (voir point 3.3). L'homme du métier, contrairement à ce que le requérant soutient, confronté au problème d'assurer la sécurité des transmissions des données entre un capteur et un enregistreur, n'a pas pour seul horizon technique les chrono tachygraphes utilisés pour les véhicules poids lourds. D'une part la description elle même se fixe un objectif plus large: celui de tout type de transmission entre un capteur délivrant des impulsions et un enregistreur chargé de les traiter (colonne 1 lignes 44 à 46 de la demande telle que publiée). Ensuite les problèmes de sécurité posés par la transmission dans un chrono tachygraphe font appel à des connaissances communes aux transmissions de messages que l'on veut protéger de tout sabotage; l'homme du métier, pour résoudre le problème de sécurité des transmissions dans un tachygraphe, ne pouvait pas ne pas élargir ses recherches au domaine technique des transmissions en général dont le document D2 fait partie.

3.2 Nouveauté

Le procédé selon la revendication 1 diffère de celui divulgué par D2 entre autre par la réinitialisation des codes de chiffrement à la suite d'une commande transmise

par l'enregistreur dans le message de commande. C'est-à-dire que les codes utilisés pour le chiffrement et le déchiffrement des messages dans le module enregistreur d'une part et le module capteur d'autre part sont changés de temps en temps. Une autre différence consiste dans le fait que le capteur est un capteur tachymétrique. L'objet de la revendication 1 est donc nouveau.

3.3 Activité inventive

Le problème à la base de la revendication 1 est de créer un procédé pour la sécurisation de la transmission des données entre un capteur délivrant des signaux et un enregistreur traitant ceux-ci, qui convienne aux contraintes physiques données dans un chrono tachygraphe, qui soit susceptible de rendre toute falsification de capteurs ou de données impossible et par lequel la sécurité de la transmission soit atteinte avec un effort réduit.

Dans le procédé selon la revendication 1, les codes utilisés pour le chiffrement et le déchiffrement sont changés de temps en temps. Par ce moyen, la sécurité de la transmission est augmentée, car l'effort pour trouver les codes modifiés perpétuellement est considérablement augmenté. Les codes peuvent être changés à une fréquence telle que le temps nécessaire pour trouver un code particulier actuel dépasse la durée pendant laquelle le code particulier est utilisé. De cette façon la sécurité de la transmission avec un code d'une longueur donnée est augmentée par rapport à celle de la transmission avec seulement un code de la même longueur, qui n'est pas changé.

Dans le procédé divulgué par D2, il n'est prévu que des différents algorithmes pour le chiffrement et le déchiffrement dans les deux directions. L'algorithme de chiffrement ou de déchiffrement agit au même niveau que le code de chiffrement. Aucune indication ne peut être trouvée dans D2 de changer l'algorithme du chiffrement. La seule chose qui est renouvelée périodiquement dans le procédé selon D2 sont les "seed numbers" (graines) à la base desquels les nombres aléatoires sont générés qui sont ajoutés au message avant le chiffrement. Les nombres aléatoires font partie du message qui est chiffré. Une fois que la clé du chiffrement est connue, le message est accessible et les nombres aléatoires ne le protègent pas. La mesure de renouveler la base de chiffres pour générer des nombres aléatoires n'augmente donc pas la sécurité du chiffrement. Aucune indication peut être trouvée dans D2 de modifier l'algorithme ou la clé du chiffrement.

En plus, en prévoyant la possibilité de réinitialiser le code de chiffrement et de déchiffrement à la suite d'une commande transmise par le module enregistreur, la possibilité est donnée de remplacer le module enregistreur sans remplacer le module capteur. Par la commande de réinitialisation de code, le module capteur peut être opéré en utilisant un autre code.

Ces possibilités ne se présentent pas dans le procédé divulgué par D2, puisque le module enregistreur et le module capteur sont réalisés en paire qui doit être changée en une fois. En remplaçant seulement un des modules, par exemple le module capteur, une alerte est produite.

D2 ne contient donc aucune indication en direction de réinitialiser les codes de chiffrement et de déchiffrement. Cette mesure implique donc une activité inventive.

L'objet de la revendication 1 est donc brevetable.

La revendication 8 concerne un système adapté au procédé selon la revendication 1. Les arguments pour l'activité inventive de la revendication 1 s'appliquent *mutatis mutandis*.

Dispositif

Par ces motifs, il est statué comme suit :

1. La décision objet du recours est annulée.

2. L'affaire est renvoyée devant le département de première instance afin de délivrer un brevet sur le fondement des documents suivants déposés à l'audience:
   - revendications 1 - 9 de la requête principale
   - pages 1 - 6 de la description
   - dessins 1, 2a, 2b.

Le greffier : La Présidente :

K. Götz M.-B. Tardo-Dino