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 20 juillet 2006

N° du recours : T 0436/05 - 3.4.03

N° de la demande : 90403101.0

N° de la publication : 0427601

C.I.B. : G07F 7/10

Langue de la procédure : FR

Titre de l'invention :
Procédé d'authentification d'une carte à microprocesseur, et système le mettant en oeuvre

Titulaire du brevet :
THOMSON R&D France SNC

Opposant :
GIESECKE & DEVRIENT GmbH

Référence :
-

Normes juridiques appliquées :
CBE Art. 123(2) et (3), 56

Mot-clé :
"Reformatio in pejus"
"Activité inventive - oui"
"Extension de l'objet de la demande - non"

Décisions citées :
G 0001/99

Exergue :
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

N° du recours : T 0436/05 - 3.4.03

D E C I S I O N
de la Chambre de recours technique 3.4.03
du 20 juillet 2006

Requérante : GIESECKE & DEVRIENT GmbH
(Opposant) Prinzregentenstraße 159
D-81677 München (DE)

Mandataire : -

Intimée : THOMSON R&D France SNC
(Titulaire du brevet) 46 Quai Alphonse Le Gallo
F-92100 Boulogne-Billancourt (FR)

Mandataire : Ruellan-Lemonnier, Brigitte
THOMSON multimedia
46 quai A. Le Gallo
F-92648 Boulogne Cédex (FR)

Décision attaquée : **Décision intermédiaire de la division d'opposition de l'Office européen des brevets postée le 22 mars 2005 concernant le maintien du brevet européen n° 0427601 dans une forme modifiée.**

Composition de la Chambre :

Président : R. G. O'Connell
Membres : V. L. P. Frank
J. Van Moer

Exposé des faits et conclusions

I. Un recours a été formé par l'opposant en tant que seul requérant à l'encontre de la maintenance du brevet européen n° 427 601 sous la forme modifiée selon la requête subsidiaire soumise à la division d'opposition.

L'opposant a formé opposition en demandant la révocation du brevet européen dans sa totalité à cause de l'absence de nouveauté (article 54 CBE) et d'activité inventive (article 56 CBE), en application de l'article 100a) CBE.

Les antériorités suivantes furent citées entre autres au cours de la procédure d'opposition :

D1 : EP 0 137 999 A

D2 : EP 0 335 768 A

II. La teneur des revendications indépendantes 1 et 6 maintenues par la division d'opposition est la suivante :

> "1. Procédé d'authentification de cartes à microprocesseur dans un système comportant au moins un centre de gestion et/ou de contrôle et/ou de distribution de prestations relié à au moins un terminal comprenant au moins un lecteur de cartes à microprocesseur, ledit procédé comportant l'étape d'authentification de cartes, ledit procédé étant caractérisé par le fait
> qu'il consiste à faire effectuer à la carte ou aux cartes de chaque terminal, pendant au moins une partie du temps pendant lequel une carte y est insérée ou des cartes y sont insérées, au moins une

opération d'authentification, ladite opération d'authentification étant commandée par des messages produits de manière irrégulière par le centre de gestion."

"6. Système d'authentification de cartes à microprocesseur comportant au mains un centre de gestion (1) et au moins un terminal (2) comprenant au moins un lecteur de cartes à microprocesseur, le lecteur du terminal comportant des moyens (4') de commande de production de signaux d'authentification et des moyens d'analyse de réponse des cartes utilisées (5), caractérisé en ce que
le terminal comporte des moyens d'inhibition et/ou de dévalidation de carte et en ce que
le centre de gestion comporte un circuit (1') produisant de manière irrégulière des messages de commande d'opérations d'authentification pour faire effectuer au moins une opération d'authentification à la ou aux cartes de chaque terminal pendant au moins une partie du temps pendant lequel une ou des cartes sont insérées."

III. La division d'opposition a estimé que les revendications selon la requête subsidiaire satisfaisaient aux exigences de l'article 123(2) CBE, car la demande telle que déposée divulgue que les messages sont émis, de préférence irrégulièrement, par l'émetteur. Elle a conclu par conséquent que l'expression modifiée "des messages produits de manière irrégulière par le centre de gestion" ne représentait pas un enseignement qui dépasserait le contenu de la demande telle que déposée.

En outre, la division d'opposition a estimé que la revendication 1 selon la requête subsidiaire différait du procédé selon Dl en ce que les messages sont produits par le centre de gestion **de manière irrégulière**, car le document Dl décrivait des transactions financières effectuées par un utilisateur au moyen d'un terminal point de vente pour lesquelles une seule opération d'authentification par transaction était nécessaire. La méthode d'authentification selon le document Dl concernait à la fois l'authentification du porteur de carte grâce à la saisie d'un code PIN et l'authentification de la carte elle même (paramètre KP). Les opérations d'authentification décrites dans Dl faisaient donc toujours intervenir le PIN dans le calcul des messages échangés entre la carte, le terminal et le centre de gestion. De l'avis de la division d'opposition, il n'y avait pas de raison, dans le cadre de ce type de transactions, de procéder à plusieurs opérations d'authentification pendant le déroulement d'une même transaction puisque la méthode d'authentification faisait toujours intervenir le code PIN et que celui-ci n'était saisi qu'une seule fois par l'utilisateur au cours d'une même transaction.

La division d'opposition a donc conclu que le problème que l'invention se proposait de résoudre était celui de l'augmentation de la sécurité des procédures d'authentification de cartes.

Elle a estimé qu'à partir du type de transactions mises en œuvre dans Dl, il n'y aurait pas lieu de procéder à plusieurs opérations d'authentification espacées dans le temps, comme c'était le cas dans le contexte de la télévision à péage, au sein d'une même transaction. Il

n'aurait pas été évident pour l'homme du métier de considérer l'incorporation de plusieurs messages produits de manière irrégulière au procédé décrit dans le document Dl afin de rendre plus sures les transactions considérées. De plus, la production (au sens de l'émission) de messages par le centre de gestion de manière irrégulière, conférait au procédé un caractère aléatoire qui en augmentait la sécurité générale. Pour ces raisons la division d'opposition a conclu que les objets des revendications 1 et 6 selon la requête subsidiaire étaient nouveaux et inventifs par rapport à l'enseignement de Dl et aux connaissances de l'homme du métier.

IV. Au cours de la procédure orale devant la chambre de recours l'intimé et titulaire du brevet a déposée une nouvelle requête principale et des requêtes subsidiaires 1 et 2. La seule modification apportée à la requête principale par rapport aux revendications maintenues par la division d'opposition a été le remplacement au troisième alinéa de la revendication 6 de l'expression "le centre de gestion comporte un circuit (1') **produisant** de manière irrégulière des messages de commande d'opérations d'authentification" par l'expression "le centre de gestion comporte un circuit (1') **émettant** de manière irrégulière des messages de commande d'opérations d'authentification".

La teneur des revendications indépendantes 1 et 6 selon la requête principale est donc la suivante :

"1. Procédé d'authentification de cartes à microprocesseur dans un système comportant au moins un centre de gestion et/ou de contrôle et/ou de

distribution de prestations relié à au moins un terminal comprenant au moins un lecteur de cartes à microprocesseur, ledit procédé comportant l'étape d'authentification de cartes, ledit procédé étant caractérisé par le fait
qu'il consiste à faire effectuer à la carte ou aux cartes de chaque terminal, pendant au moins une partie du temps pendant lequel une carte y est insérée ou des cartes y sont insérées, au moins une opération d'authentification, ladite opération d'authentification étant commandée par des messages produits de manière irrégulière par le centre de gestion."

"6. Système d'authentification de cartes à microprocesseur comportant au moins un centre de gestion (1) et au moins un terminal (2) comprenant au moins un lecteur de cartes à microprocesseur, le lecteur du terminal comportant des moyens (4') de commande de production de signaux d'authentification et des moyens d'analyse de réponse des cartes utilisées (5), caractérisé en ce que
le terminal comporte des moyens d'inhibition et/ou de dévalidation de carte et en ce que
le centre de gestion comporte un circuit (1') émettant de manière irrégulière des messages de commande d'opérations d'authentification pour faire effectuer au moins une opération d'authentification à la ou aux cartes de chaque terminal pendant au moins une partie du temps pendant lequel une ou des cartes sont insérées."

V. Le requérant opposant a essentiellement développé les arguments suivants :

– La revendication 6 telle que modifiée pendant la procédure d'opposition ne satisfait pas aux exigences de l'article 123(2) CBE, car la demande telle qu'elle avait été déposée divulgue seulement que le centre de gestion comporte un circuit **émettant** les messages d'authentification de manière irrégulière. Il n'y avait aucune mention d'un circuit **produisant** ces messages de manière irrégulière.

– Par ailleurs, la modification apportée à la revendication 6 de la requête principale pendant la procédure orale devant la chambre de recours pour satisfaire aux exigences de l'article 123(2) CBE ne devrait pas être permise, car elle allait à l'encontre du principe de l'interdiction de la *reformatio in pejus.* Le titulaire du brevet et intimé était censé défendre le brevet tel qu'approuvé par la division d'opposition dans sa décision intermédiaire. L'acquiescement à la modification placerait l'opposant et unique requérant dans une situation plus défavorable que s'il n'avait pas formé de recours. Par ailleurs, la modification de la revendication 6 étendrait la protection du brevet (article 123(3) CBE).

– Le procédé d'authentification selon la revendication 1 différait du procédé divulgué au document D1 en ce que ladite authentification était commandée par des messages produits de manière irrégulière par le centre de gestion. Cependant, l'homme du métier savait de façon générale effectuer

des contrôles de manière aléatoire. Comme dans un système de télévision à péage la carte restait longtemps insérée dans le terminal, il était évident pour l'homme du métier d'authentifier la carte plusieurs fois soit à de très courts intervalles soit de façon aléatoire. En conséquence le procédé selon la revendication 1 n'impliquait pas une activité inventive.

VI. L'intimé et titulaire du brevet a essentiellement développé les arguments suivants :

– La modification apportée aux revendications indépendantes 1 et 6 pendant la procédure d'opposition consistant à insérer la caractéristique "de manière irrégulière" ne contrevient pas aux dispositions de l'article 123(2) CBE. Il ressort de la demande telle que déposée que "l'émetteur 1 diffuse sous la commande d'un circuit 1',..., des messages d'authentification" et "que les messages émis, de préférence irrégulièrement par l'émetteur 1" commandent au lecteur de carte de faire effectuer à la carte au moins deux opérations combinatoires pour l'authentification de la carte. La demande telle que déposée divulgue donc que le centre de gestion (et plus précisément un circuit 1' du centre de gestion) produit des messages de commande d'opération d'authentification et ces messages sont émis de manière irrégulière par le centre de gestion. Comme le but de ces messages produits par le centre de gestion est de déclencher une opération d'authentification de la carte, ces messages sont nécessairement produits et immédiatement émis par le centre de gestion. La formulation des revendications

1 et 6 selon laquelle les messages de commande de l'opération d'authentification sont produits de manière irrégulière par le centre de gestion est donc équivalente à la formulation de la demande telle que déposée.

– L'objet du brevet est un procédé d'authentification de cartes à microprocesseur dans un système comportant au moins un centre de gestion relié à un terminal comprenant un lecteur de cartes à microprocesseur. Cette invention a été développée dans le contexte de la télévision à péage pour détecter des cartes non valides ou des simulateurs de cartes fabriqués par des pirates. Un aspect important de l'invention est de faire effectuer à une carte insérée dans un terminal des opérations d'authentification sur commande de messages produits par un centre de gestion distant et ce, de manière imprévisible puisque ces messages sont produits de manière irrégulière. Le déclenchement des opérations d'authentification n'est donc pas maitrisé localement au niveau du terminal mais à distance, par le centre de gestion.

– Le document Dl décrit un système de transfert de fonds électroniques comprenant des centres de traitement de données d'agences de distribution de cartes reliés par un réseau de communication à des contrôleurs de magasins qui sont eux-mêmes connectés à des terminaux de transaction, lesquels comportent des moyens d'entrée/sortie pour communiquer avec une carte à microprocesseur. Le document Dl décrit un procédé mis en œuvre par ce système visant à vérifier la validité d'un code personnel (PIN) entré par un

utilisateur lors d'une transaction ayant pour but un transfert de fond. Ce document vise à vérifier la validité d'un code d'identification personnel (PIN) localement, au sein d'un terminal utilisé pour les transactions, sans avoir besoin d'envoyer ce PIN à un centre de contrôle distant. C'est en effet l'avantage principal de l'invention décrit dans D1. Ces étapes portent effectivement sur un procède de vérification da la validité d'un code PIN et non sur une authentification de carte.

– En outre le document D2 n'enseigne pas une authentification de carte pour la simple raison que ce n'est pas une carte à microprocesseur. C'est une carte prépayée destinée à la téléphonie. Le but de la procédure cryptographique est d'authentifier qu'un élément de paiement a été grillé et non d'authentifier la carte.

VII. À la procédure orale devant la chambre de recours le requérant opposant a demandé l'annulation de la décision attaquée et la révocation du brevet.

L'intimé et titulaire du brevet a demandé le rejet du recours et le maintien du brevet sur la base de la requête principale déposée à la procédure orale le 20 juillet 2006 ou sur la base d'une première ou une deuxième requête subsidiaire déposées à la procédure orale.

Requête principale :
Description :
colonnes 1 et 2 telles que déposées à la procédure orale

colonnes 3 et 4 telles que maintenues par la division d'opposition

Revendications :

1 à 7 déposées à la procédure orale

Figure unique telle que maintenue par la division d'opposition

Requête subsidiaire 1 :

Revendications :

1 à 7 déposées à la procédure orale

Requête subsidiaire 2 :

Revendications :

1 à 7 déposées à la procédure orale

Motifs de la décision

1. Le recours est recevable.

2. *Requête principale - Article 123(2) et (3) CBE*

2.1 La requérante opposante a fait valoir que la demande telle que déposée ne divulgue pas un circuit produisant de manière irrégulière des messages de commande d'opérations d'authentification comme spécifié à la revendication indépendante 6, seulement l'émission irrégulière de ces messages étant divulguée (voir page 3, ligne 30 de la demande telle que déposée). En outre, la production d'un message n'était pas équivalente à l'émission d'un message, car un message peut être produit sans être nécessairement émis.

2.2 L'intimé et titulaire du brevet a argumenté que le but des messages produits par le centre de gestion est de déclencher une opération d'authentification de la carte, ces messages sont donc nécessairement produits et immédiatement émis par le centre de gestion.

2.3 La chambre considère que les procédures de production et d'émission d'un message sont des pas logiquement différents et temporellement séparées, car la production d'un message précède son émission. En outre, une production des messages de manière irrégulière n'implique pas une émission de manière irrégulière ni vice versa. Il s'en suit que le système d'authentification selon la revendication 6 telle que maintenue par la division d'opposition va à l'encontre des dispositions de l'article 123(2) CBE.

2.4 Par contre la revendication 6 telle que déposée à la procédure orale devant la chambre de recours indique que "le centre de gestion comporte un circuit (1') **émettant** de manière irrégulière des messages de commande d'opérations d'authentification". Ceci est divulgué au brevet par la spécification que les messages sont **émis**, de préférence irrégulièrement, par l'émetteur 1 ([0017] du brevet publié) et que l'émetteur 1 diffuse sous la commande d'un circuit 1' … des messages d'authentification (ibid. [0015]).

2.5 En outre, le remplacement de l'expression "le centre de gestion comporte un circuit (1') **produisant** de manière irrégulière des messages de commande d'opérations d'authentification" par l'expression "le centre de gestion comporte un circuit (1') **émettant** de manière

irrégulière des messages de commande d'opérations d'authentification" réduits la protection du brevet, car l'émission d'un message requiert *à fortiori* la production de cet message. Par contre, un message qui a été produit n'est pas nécessairement émis.

2.6 Les modifications apportées au brevet n'introduisent donc pas de matière additionnelle et la protection du brevet ne s'en trouve pas étendue. Ces modifications ne vont donc pas à l'encontre des dispositions de l'article 123(2) et (3) CBE.

3. *Recevabilité de la requête principale*

3.1 L'opposant et seule requérant avait fait valoir que les modifications apportées au brevet iraient à l'encontre du principe de l'interdiction de la *reformatio in pejus*, car il serait placé dans une situation plus défavorable que s'il n'avait pas formé de recours.

3.2 Cette situation a été à la base de la décision G 1/99 (JO OEB 2001, 381) de la Grande Chambre de Recours. Le dispositif de cette décision est libellé comme suit :

> *"En principe, il convient de rejeter une revendication modifiée qui placerait l'opposant et unique requérant dans une situation plus défavorable que s'il n'avait pas formé de recours. II peut néanmoins être fait exception à ce principe afin de répondre à une objection soulevée par l'opposant/requérant ou par la chambre au cours de la procédure de recours, si le brevet tel que maintenu sous une forme modifiée devait sinon être révoqué,*

cette révocation étant la conséquence directe d'une modification irrecevable que la division d'opposition avait admise dans sa décision intermédiaire.

Dans de telles circonstances, le titulaire du brevet/intimé peut être autorisé, afin de remédier à cette situation, à présenter les requêtes suivantes :

- *en premier lieu une requête en modification visant à introduire une ou plusieurs caractéristiques initialement divulguées qui limitent la portée du brevet tel que maintenu ;*

- *si une telle limitation s'avère impossible, une requête en modification visant à introduire une ou plusieurs caractéristiques initialement divulguées qui étendent la portée du brevet tel que maintenu, mais dans les limites de l'article 123(3) CBE ;*

- *en fin, si de telles modifications s'avèrent impossibles, une requête tendant à la suppression de la modification irrecevable, mais dans les limites de l'article 123(3) CBE."*

3.3 Comme analysé au point 2.5 ci-dessus la modification apportée au brevet (c.a.d. le remplacement de l'expression "produisant" par "émettant" à la revendication 6) limite la portée du brevet tel que maintenu. C'est donc une modification qui est en accord avec les modifications à faire en premier lieu selon la décision G 1/99. La requête principale est donc recevable.

4. *Requête principale – Activité inventive (article 56 CBE)*

4.1 Le document D1 décrit un système de transfert de fonds électronique comprenant des centres de gestion 10 reliés par un réseau de communication à des terminaux de transactions 18. Dans ce système le code d'identification personnelle (PIN) entré par l'utilisateur au terminal est utilisé pour générer un paramètre d'authentification de transaction (TAPc) en utilisant en plus le code secret de la carte (KP). Le TAPc est généré en réponse à un message du centre de gestion (Mresp) reçue par le terminal (page 8 et Figure 1). Cependant, l'authentification du porteur de la carte est faite une seule fois au début même de la transaction.

4.2 Le procédé d'authentification de cartes à microprocesseur selon la revendication 1 diffère donc du procédé décrit au document D1 en ce que ladite authentification est commandée par des messages produits de manière irrégulière par le centre de gestion. Ceci a pour but d'augmenter la sécurité des procédures d'authentification de cartes.

4.3 Le requérant opposant avait fait valoir que cette différence n'impliquait pas une activité inventive pour l'homme du métier car dans un système de télévision à péage, dans lequel la carte à microprocesseur restait longtemps dans le terminal, il aurait été évident d'authentifier la carte plusieurs fois pendant son utilisation. Cette authentification pouvait être faite de manière régulière ou irrégulière.

4.4 La chambre ne peut cependant partager cet avis, car rien dans le document D1 ne laisse supposer que la procédure cryptographique se déroulant entre la carte, le terminal et le centre de gestion puisse varier d'une transaction à une autre ou que la vérification de la carte puisse être faite plusieurs fois, soit de façon régulière soit de façon irrégulière, pendant la même transaction.

4.5 De plus, le document D2 n'incite pas l'homme du métier de déclencher des opérations d'authentification de façon irrégulière, car il décrit un système de paiement pour communications téléphoniques en utilisant une carte prépayée dans lequel le module de contrôle 108 calcule une valeur d'authentification K_i à chaque impulsion de taxation de la communication qui est comparée avec la valeur précédente K'_i. Si elles ne sont pas identiques ou correspondantes, la ligne téléphoniques est inhibée (colonne 3, lignes 34 à 43). En conséquence, les messages déclenchant une authentification d'une unité téléphonique écoulée interviennent à des moments réguliers et sont donc parfaitement prévisibles.

4.6 La production et l'émission de messages par le centre de gestion de manière irrégulière confère au procédé d'authentification de la carte un caractère aléatoire qui en augmente la sécurité générale.

4.7 Les raisons exposées ci-dessus s'appliquent de la même manière au procédé d'authentification selon la revendication 1 comme au système d'authentification selon la revendication 6. Les objets des revendications 1 et 6 sont donc considérées comme impliquant une activité inventive au sens de l'article 56 CBE.

5. En conséquence, la chambre juge que le brevet dans la version de la requête principale satisfait aux conditions de la CBE.

Dispositif

Par ces motifs, il est statué comme suit :

1. La décision attaquée est annulée.

2. L'affaire est remise à la première instance avec l'ordre de maintenir le brevet dans la version suivante :

Description :

colonnes 1 et 2 telles que déposées à la procédure orale
colonnes 3 et 4 telles que maintenues par la division d'opposition

Revendications :

1 à 7 selon la requête principale déposée à la procédure orale

Figure unique telle que maintenue par la division d'opposition

La Greffière : Le Président :

S. Sánchez Chiquero R. G. O'Connell