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 23 octobre 2008

N° du recours : T 0277/06 - 3.4.03

N° de la demande : 01940645.3

N° de la publication : 1290647

C.I.B. : G07F 7/10

Langue de la procédure : FR

Titre de l'invention :
Procédé de cryptographie et microcircuit pour carte à puce

Titulaire du brevet :
FRANCE TELECOM

Opposant :
GIESECKE & DEVRIENT GmbH

Référence :
-

Normes juridiques appliquées (CBE 1973) :
CBE Art. 56

Mot-clé :
"Activité inventive (non)"

Décisions citées :
-

Exergue :
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

N° du recours : T 0277/06 - 3.4.03

D E C I S I O N
de la Chambre de recours technique 3.4.03
du 23 octobre 2008

(Opposant) GIESECKE & DEVRIENT GmbH
Prinzregentenstr. 159
D-81677 München (DE)

Mandataire : -

Intimée : FRANCE TELECOM
(Titulaire du brevet) 6, Place d'Alleray
F-75015 Paris (FR)

Mandataire : Santarelli
14, avenue de la Grande Armée
B.P. 237
F-75822 Paris Cedex 17 (FR)

Décision attaquée : **Décision intermédiaire de la division d'opposition de l'Office européen des brevets postée le 31 janvier 2006 concernant le maintien du brevet européen n° 1290647 dans une forme modifiée.**

Composition de la Chambre :

Président : V. L. P. Frank
Membres : R. Q. Bekkering
J. Van Moer

Exposé des faits et conclusions

I. Le recours a été formé par l'opposante à l'encontre de la décision intermédiaire de la division d'opposition de maintenir le brevet tel qu'il a été modifié.

II. La requérante demande l'annulation de la décision intermédiaire de la division d'opposition et la révocation du brevet dans son ensemble.

III. L'intimée (titulaire du brevet) demande le rejet du recours.

IV. La revendication 1 s'énonce comme suit :

"*1. Procédé de cryptographie comprenant des étapes de calcul cryptographique mis en œuvre par une carte à puce(s) comprenant une unité centrale, ledit procédé comprenant en outre une ou plusieurs étapes de précalculs réalisées par la carte à puce(s) elle-même, caractérisé en ce que la ou lesdites étapes de précalculs sont réalisées lors d'une session opérée par la carte à puce et pendant des périodes d'attente d'entrées-sorties de son unité centrale.*"

V. Référence est faite aux documents suivants :

D1 : B. Schneier, "Angewandte Kryptographie", Addison Wesley, 1996, pages 553 - 561

D2 : WO 99 01960 A

VI. La requérante a essentiellement argué comme suit :

L'objet de la revendication 1 n'impliquait pas une activité inventive par rapport au document D1 et les connaissances générales de l'homme du métier confirmées par le document D2.

Le document D1 divulguait un procédé de cryptographie comprenant des étapes de calcul cryptographique mis en œuvre par une carte à puce avec une unité centrale. Le procédé comprenait des étapes de précalculs réalisées par la carte à puce elle-même. Vu que la carte elle-même n'avait pas d'alimentation en énergie, mais était uniquement alimentée par le terminal pendant une session avec celui-ci, toutes étapes de calculs ou de précalculs par la carte étaient forcement réalisées par la carte lors d'une session opérée par la carte à puce tel que défini à la revendication 1.

Par contre, le document D1 ne spécifiait pas explicitement le moment ou la carte exécutait ces étapes de précalculs.

Le problème objectif à résoudre pouvait donc être formulé comme suit : quand réaliser les étapes de précalculs lors d'une session opérée par la carte.

La seule possibilité d'obtenir une accélération du procédé cryptographique d'authentification, tel qu'indiquée dans le document D1, était de réaliser ces étapes de précalculs pendant des périodes pendant lesquelles l'unité centrale était inactive et donc forcément pendant des périodes d'attente d'entrées-sorties de l'unité centrale.

De plus, le document D2 confirmait pour l'homme du métier la faisabilité d'une telle solution. En particulier, D2 divulguait un procédé de cryptographie dans lequel une carte à puce continuait le traitement normal pendant des périodes d'attente dans la communication entre la carte et un terminal.

VII. L'intimée a essentiellement présenté les arguments suivants :

L'objet de la revendication 1 impliquait une activité inventive par rapport aux documents D1 et D2. Bien que le document D1 divulguait un procédé de cryptographie comprenant des étapes de calcul cryptographique mis en œuvre par une carte à puce avec une unité centrale conformément au préambule de la revendication 1, il n'y avait aucune indication dans le document D1 sur la réalisation des étapes de précalculs lors d'une session opérée par la carte à puce et pendant des périodes d'attente d'entrées-sorties de son unité centrale.

Contrairement à ce qui était soutenu par la requérante, d'autres solutions étaient effectivement possibles tout en garantissant une accélération du procédé cryptographique. En particulier, il était imaginable de calculer plusieurs témoins en avance et de les stocker sur la carte, bien avant la transaction avec le terminal. Cela permettait également d'accélérer les transactions successives. En conséquence, la réalisation des étapes de précalculs pendant des périodes d'attente d'entrées-sorties de l'unité centrale de la carte ne pouvait pas résulter de façon implicite de D1 non plus.

En ce qui concernait le document D2, ce document ne traitait pas d'un procédé de cryptographie comprenant des précalculs et ne pouvait pas donc aider dans la solution du problème objectif relatif à D1 à savoir comment réaliser les étapes de précalculs.

Motifs de la décision

1. Le recours est recevable.

2. *Activité inventive*

2.1 Le document D1 divulgue un procédé de cryptographie comprenant des étapes de calcul cryptographique mis en œuvre par une carte à puce avec une unité centrale (voir page 553, dernier paragraphe). Le procédé comprend des étapes de précalculs réalisées par la carte à puce elle-même (voir page 555, section 3, deuxième paragraphe ; page 557, dernier paragraphe ; page 558, premier paragraphe ; page 559, tableau 20.3). En particulier, les calculs réalisés hors de la carte étant indiqués dans le tableau 20.3 susmentionné, il est implicite que les étapes de précalculs ("Vorausberechnungen") en question soient réalisées par la carte à puce elle-même.

Toutes les caractéristiques du préambule de la revendication 1 sont donc connues du document D1.

Restent les deux caractéristiques suivantes de la partie caractérisante de la revendication 1 :

a) *la ou lesdites étapes de précalculs sont réalisées lors d'une session opérée par la carte à puce et*

b) pendant des périodes d'attente d'entrées-sorties de son unité centrale.

2.2 Au sujet des caractéristiques susmentionnées, la requérante a argumenté que, vu que la carte elle-même n'avait pas d'alimentation en énergie mais était alimentée par le terminal durant la session avec la dernière, tous calculs, ou précalculs, par la carte, étaient forcement réalisés par la carte lors d'une session opérée par la carte à puce. De plus, la seule possibilité d'obtenir l'accélération du procédé cryptographique d'authentification indiquée dans le document D1, était de réaliser ces étapes de précalculs pendant des périodes dans lesquelles l'unité centrale était inactive et donc forcement pendant des périodes d'attente d'entrées-sorties de son unité centrale.

L'intimée, par contre, a soutenu, en faisant référence aux paragraphes [0055] et [0056] du brevet contesté, que dans le sens du brevet, la session opérée par la carte était une période pendant laquelle la carte travaillait de façon autonome et les étapes de précalculs étaient réalisées à l'initiative de la carte. Or, le document D1 n'était qu'un ouvrage général, théorique qui ne fournissait aucune information concrète quant au moment où les étapes de précalculs seraient réalisées. De plus, il n'y avait aucune indication dans le document D1 sur la réalisation des étapes de précalculs pendant des périodes d'attente d'entrées-sorties de l'unité centrale de la carte.

Quant à l'argument de la requérante qu'il n'y avait aucune autre possibilité d'obtenir l'accélération du

procédé cryptographique d'authentification indiquée dans le document D1, l'intimée a fait valoir que d'autres solutions étaient effectivement possibles tout en garantissant une accélération du procédé cryptographique. Comme indiqué dans le brevet (paragraphe [0022]), il était connu de précalculer des témoins à utiliser lors de la procédure de signature dans des sessions de transaction successives et de les stocker sur la carte. Ces précalculs étaient faits par un organe extérieur. Il était toutefois imaginable de faire faire ces précalculs par la carte elle-même. Il suffisait dans ce but de prévoir un terminal de recharge fournissant l'alimentation en énergie de la carte et permettant à la carte de précalculer un stock de témoins. Cela permettrait également d'accélérer les transactions successives. En conséquence, la réalisation des étapes de précalculs pendant des périodes d'attente d'entrées-sorties de l'unité centrale de la carte ne pouvait pas résulter de façon implicite de D1 non plus.

2.3 La chambre est d'accord avec l'intimée sur ce point. Le document D1 se rapporte à un procédé cryptographique DSA (Digital Signature Algorithm), un algorithme à clé publique, qui prévoit la génération d'une signature avec une clé privée par l'émetteur, une carte à puce, et la vérification de l'authenticité de la signature avec une clé publique par le récepteur. Le procédé permet de calculer en avance certaines valeurs nécessaires pour la génération de la signature par la carte. En fait, le brevet contesté concerne un procédé cryptographique de ce type et prévoit le précalcul de ces valeurs dites "témoins".

Bien que ces précalculs soient indiqués dans D1, rien de concret n'est divulgué sur le moment où faire ces précalculs. Dans D1, la seule information supplémentaire à cet égard est que le but des précalculs est d'accélérer le procédé, c'est-à-dire la génération de la signature par la carte.

Or, effectivement, de l'avis de la chambre il est envisageable de calculer à l'avance ces "témoins" hors d'une session avec des entrées-sorties de la carte. En particulier, dans ce cas un terminal fournit l'alimentation en énergie de la carte sans qu'il y ait des entrées-sorties de la carte ou des périodes d'attente d'entrées-sorties correspondantes.

En conséquence, de l'avis de la chambre, dans le document D1 les caractéristiques susmentionnées de la partie caractérisante de la revendication 1 ne sont divulguées ni de façon explicite, ni de façon implicite.

2.4 De surcroît, l'intimée a argumenté que le document D1 ne pouvait guère être un point de départ approprié pour l'homme du métier en ce qui concernait les précalculs. Le temps nécessaire pour faire les précalculs selon D1 était de 14 secondes, ce qui était beaucoup trop long pour l'application envisagée dans le brevet (durée totale de l'ordre de 150 ms). L'homme du métier aurait donc aussi écarté ce document pour cette raison.

Toutefois, la chambre ne peut pas être d'accord avec l'intimée à cet égard. Le brevet traite aussi d'un exemple d'application relatif à une carte porte-monnaie électronique avec un temps d'attente de la carte de l'ordre de 15 secondes (voir paragraphe [0030]). La

durée des précalculs de D1 de 14 secondes ou même 4 secondes (DSA avec paramètres communs (voir tableau 20.3)) indiquée est bien compatible avec une telle application.

De l'avis de la chambre le document D1 est donc clairement pertinent et constitue l'art antérieur le plus proche.

2.5 Au vu des différences entre l'objet de la revendication 1 et le document D1 mentionnées ci-dessus, le problème objectif à résoudre relatif au document D1 peut donc être formulé comme suit : décider quand réaliser les précalculs.

Dans la solution il est cependant à prendre en considération que, bien que le document D1 concerne l'accélération du procédé cryptographique d'authentification en soi, il est évident que finalement l'objectif est une accélération de la transaction effectuée avec la carte comprenant ce procédé cryptographique.

De l'avis de la chambre, il est évident pour un homme du métier qui travaille dans le domaine de la cryptographie pour cartes à puce, que les précalculs ne peuvent se faire que soit avant la transaction avec la carte, soit pendant cette transaction.

La première alternative, arguée par l'intimée, comporte toutefois des inconvénients évidents pour l'homme du métier, car elle comprend une étape supplémentaire, qui prend du temps et nécessite de l'équipement supplémentaire.

L'homme du métier est donc incité à chercher la solution dans le cadre de la transaction elle même.

Selon la chambre, il est évident pour l'homme du métier de considérer à cette fin les périodes d'inactivité de l'unité centrale de la carte à puce. Utiliser les temps morts d'une application pour faire exécuter une autre application est tout d'abord un principe généralement appliqué dans le domaine des microprocesseurs. De plus, le document D2 montre que dans le domaine spécifique des cartes à puce pour des procédés cryptographiques, il est connu de faire continuer le traitement par la carte pendant les temps morts pendant la communication entre la carte et le terminal correspondant (voir page 11, ligne 4 à la page 13, ligne 15). En conséquence, il est évident pour l'homme du métier de réaliser les étapes de précalculs pendant des périodes d'attente d'entrées-sorties de son unité centrale. De plus, vu que la carte à puce avec son unité centrale est tout à fait capable d'opérer de façon autonome et dispose elle-même des informations nécessaires relatives à l'occurrence de périodes d'attente d'entrées-sorties de son unité centrale, il est évident pour l'homme du métier que la façon la plus efficace de réaliser ces précalculs est lors d'une session opérée par la carte à puce.

Quant à l'argument dans la décision contestée, que le document D1 permettrait éventuellement de localiser ces précalculs dans la phase d'initialisation d'une session, il est clair qu'une telle solution ne permet pas d'accélérer la transaction et donc, de l'avis de la chambre, serait écartée par l'homme du métier.

2.6 L'objet de la revendication 1 découle donc pour l'homme du métier de manière évidente de l'état de la technique et en conséquence n'implique pas une activité inventive (Article 56 CBE 1973).

Dispositif

Par ces motifs, il est statué comme suit :

1. La décision attaquée est annulée.

2. Le brevet est révoqué.

Le Greffier : Le Président :

S. Sánchez Chiquero V. L. P. Frank