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) [X] Aux Présidents

D E C I S I O N
du 23 juin 1993

N° de recours: T 0304/92 - 3.5.1

N° de la demande: 82401752.9

N° de la publication: 0077238

IPC: H04L 9/00

Langue de la procédure: FR

Titre de l'invention:
Procédé et dispositif pour authentifier la signature d'un message signé

Demandeur/Titulaire du brevet:
BULL S.A.

Opposant:
GAO Gesellschaft für Automation und Organisation mbH

Référence:

Normes juridiques relevantes:
CBE Art. Art. 52(1), 56

Mot-clé:
"Activité inventive (non)"

Décisions citées:
T 598/88, T 153/85, T 95/83, T 33/91, T 166/86, T 38/89, T 406/86

Exergue:

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

N°. du recours : T 0304/92 - 3.5.1

D E C I S I O N
de la Chambre de recours technique 3.5.1
du 23 juin 1993

Requérant : (Opposant)
GAO Gesellschaft für Automation und Organisation mbH
Euckenstraße 12
W - 8000 München 70 (DE)

Mandataire :
Klunker, Schmitt-Nilson, Hirsch
Winzererstraße 106
W - 8000 München 40 (DE)

Adversaire : (Titulaire du brevet)
BULL S.A.
121, Avenue de Malakoff
F - 75116 Paris (FR)

Mandataire :
Debay, Yves
BULL S.A.
Tour BULL Cédex 74,
PC/TB2803
F - 92039 Paris La Défense (FR)

Décision attaquée : **Décision intermédiaire de la division d'opposition de l'Office européen des brevets du 3 février 1992 concernant le maintien du brevet n° 0 077 238 dans une forme modifiée.**

Composition de la Chambre :

Président : P.K.J. Van den Berg
Membres : C.G.F. Biggio
E.M.C. Holtz

Résumé des faits et conclusions

I. Le brevet européen EP-B1-0 077 238, basé sur la demande n° 82 401 752 déposée à l'OEB le 28 septembre 1982 et revendiquant la priorité de la demande n° 81/119 090 déposée le 9 octobre 1881 en France, fut délivréle 5 février 1986 et opposé le 4 novembre 1986.

II. Pendant la procédure d'opposition, furent prises en considération les antériorités suivantes :

D1 = EP-A-0 037 762 (mentionné dans le brevet contesté et constituant antériorité aux termes de l'article 54 (3) de la CBE),

E1 = AFIPS Conference Proceedings, Vol. 40, 1979, National Computer Conference, June 4-7, 1979, pages 831 à 837,

E2 = EP-A-0 035 448,

D2 = Michael O. Rabin : "Foundation of Secure Computation, Digitalized Signatures", 1978,

E3 = EP-A-0 028 965, et

E4 = DE-A-2 224 937.

III. Dans une notification datée du 15 mars 1991, la Division d'opposition affirma que les sujets des revendication indépendantes 1 et 4, telles que délivrées, semblaient dépourvus d'une activité inventive par rapport à l'enseignement divulgué par E1 ; cet enseignement étant lu et apprécié à la lumière de celui divulgué par D2.

Elle considéra, par contre, que les sujets des revendication indépendantes 1 et 4, telles que déposées à titre subsidiaire par la Titulaire du brevet en date du 29 mai 1987, pouvaient être considérées comme définissant une invention brevetable et suggéra des amendements aux libellés desdites revendications.

La Titulaire du brevet ayant agréé les suggestions faites par la Division d'opposition, cette dernière décida la maintenance du brevet en forme modifiée en date du 3 février 1992.

La décision était basée sur le brevet comprenant les pièces suivantes :

Description : page 2 (lignes 1 à 18 et 55 à 65), page 3 (lignes à 5 et 22 à 65), pages 4 et 5 version délivrée ;
pages 2, 3, 3bis et 5, déposées le 2 juillet 1991 ;
Revendications : 1 et 4, déposées le 2 juillet 1991 ;
2, 3, 5 à 12, version délivrée ;
Dessins : feuille 1/1 version délivrée.

IV. L'Appelante (Opposante) introduisit un recours en date du 31 mars 1992 et s'acquitta de la taxe de recours à la même date.

Les motifs du recours furent déposés en date du 3 juin 1992.

L'Appelante demanda que la décision attaquée soit annulée et que le brevet contesté soit révoqué dans sa totalité. Subsidiairement, elle demanda qu'une procédure orale soit convoquée.

V. Les observations de l'Intimée (Titulaire du brevet) furent déposées en date du 28 octobre 1992. Elle demanda que le recours soit rejeté pour les motifs déjà mentionnés dans la décision contestée.

VI. En date du 22 février 1993, par une notification aux termes de l'article 11(2) du règlement de procédure des

Chambres de recours, la Chambre convoqua les parties à une procédure orale devant avoir lieu le 22 juin 1993.

VII. En date du 18 mai 1993, au moyen d'un "telefax" ainsi daté, l'Intimée déposa un premier, un deuxième et un troisième jeux de revendications ; chacun de ces jeux comprenant un nouveau libellé des revendications indépendantes 1 et 4. Elle demanda que ces trois jeux de revendications soient pris en considération pendant la procédure orale. Elle demanda, entre outre, qu'il lui soit permis de présenter de nouvelles revendications, "au cas où aucun de ces jeux de revendications ne seraient acceptables".

VIII. Pendant la procédure orale, qui eut lieu les 22 et 23 juin 1993, l'Intimée demanda que les revendications indépendantes 1 et 4, selon le premier jeu de revendications déposé le 18 mai 1993, soient considérées comme constituant sa requête principale et que les revendications indépendantes 1 et 4, selon le troisième jeu de revendications déposé le 18 mai 1993, soient considérées comme constituant sa requête subsidiaire.

Les revendications 1 et 4, selon la requête principale, se lisent :

1. "Procédé pour authentifier l'auteur d'un message (M) signé envoyé par un appareil émetteur (1) à un appareil récepteur (3), dans lequel l'appareil émetteur crée automatiquement une signature (SG) élaborée par un programme (P) de calcul en fonction au moins du message (M), et d'une clé secrète (S) inconnue de l'émetteur du message, la vérification de l'identité de l'auteur étant faite à la demande du destinataire en utilisant au moins le message (M) et la clé secrète (S), caractérisé en ce que le message est transmis par une voie de transmission quelconque

(2), et en ce que pour vérifier l'authenticité de la signature (SG) d'un message (M) reçu par l'appareil récepteur (3), il consiste à :

- recalculer automatiquement la signature (SG) du message reçu (M) à partir d'au moins le même programme (P) précité,
- comparer automatiquement la signature (SG) du message reçu et la signature (SG) recalculée au niveau de l'appareil récepteur (3), et
- indiquer seulement au récepteur du message, le résultat égal ou différent de la comparaison précédente tout en interdisant au récepteur du message la possibilité de pouvoir prendre connaissance de la valeur de la signature recalculée".

4. "Dispositif pour la mise en oeuvre du procédé tel que défini selon l'une des revendications précédentes, comprenant un appareil émetteur (1) relié par une voie de transmission (2) à un appareil récepteur (3) pour transmettre un message (M) signé, l'appareil émetteur comprenant au moins un dispositif de mémorisation (5) dans lequel sont au moins enregistrés un programme (P) de calcul de signature et un paramètre ou clé secrète (S) inconnue de l'émetteur du message, et des circuits de traitement (6) pour élaborer automatiquement la signature (SG) du message (M) à partir du programme (P) précité qui prend en compte le contenu du message (M) et la clé secrète (S) précitée, caractérisé en ce que la voie de transmission est quelconque, et en ce que l'appareil récepteur (3) comprend au moins :

- un dispositif de mémorisation (14) dans lequel sont au moins enregistrés le programme (P) précité et la même clé secrète (S) précitée également inconnue du récepteur du message,

- des circuits de traitement (15) pour recalculer la signature (SG) d'un message reçu à partir du contenu du message, du programme (P) et de la clé secrète (S) précités,
- un dispositif de comparaison (16) dont une première entrée reçoit de l'extérieur la signature (SG) du message (M) reçu et dont la seconde entrée reçoit la signature recalculée précitée, et
- un dispositif témoin (16) à au moins deux états stables indiquant respectivement les résultats vrai ou différent de la comparaison précitée, l'entrée du dispositif témoin (16) étant reliée à la sortie du dispositif de comparaison (15)".

Les revendications 1 et 4, selon la requête subsidiaire, se lisent :

1. "Procédé pour authentifier la signature d'un message signé reçu par un appareil récepteur (3) et transmis par un appareil émetteur (1) au moyen d'une voie de transmission quelconque (2), la signature (SG) d'un message signé (M) étant élaborée automatiquement au niveau de l'appareil émetteur à partir d'un programme (P) de calcul de signature faisant au moins appel au contenu du message (M) à transmettre et à un paramètre ou clé secrète (S) inconnue de la personne émettrice du message, l'authentification de ladite signature (SG) du message (M) au niveau de l'appareil récepteur étant obtenue en recalculant automatiquement ladite signature à partir d'au moins le même programme (P), prenant en compte le contenu du message (M) reçu et la même clé secrète (S) également inconnue de la personne réceptrice du message, en comparant automatiquement la signature du message reçu à la signature recalculée au niveau de l'appareil récepteur, en indiquant à la personne

réceptrice du message le résultat égal ou différent de la comparaison, caractérisé en ce qu'il consiste :

- lors de l'élaboration de ladite signature, à insérer dans l'appareil émetteur un objet portatif (1b) dénommé carte nominative de signature, contenant au moins ledit programme (P) et ladite clé secrète (S),
- lors de l'authentification de ladite signature, à accoupler à l'appareil récepteur un objet portatif (3b), dénommé carte de contrôle accessible à plusieurs personnes, contenant au moins ledit programme (P) et ladite clé secrète (S),
- à interdire à la personne réceptrice du message la possibilité de pouvoir prendre connaissance de la valeur de la signature recalculée".

4. "Dispositif pour la mise en oeuvre du procédé tel que défini par l'une des revendications précédentes, du type constitué par un appareil émetteur (1) relié par une voie de transmission quelconque (2) à un appareil récepteur (3), l'appareil émetteur comprenant au moins un dispositif de mémorisation (5) dans lequel sont au moins enregistrés un programme (P) de calcul de signature et un paramètre ou clé secrète (S) inconnue de la personne émettrice du message, des circuits de traitements (6) pour élaborer automatiquement la signature (SG) d'un message (M) à partir du programme précité qui prend en compte le contenu du message et la clé secrète précitée, l'appareil récepteur comprenant au moins un dispositif de mémorisation (14) dans lequel sont au moins enregistrés le même programme (P) et la même clé secrète (S) également inconnue de la personne réceptrice du message, des circuits de traitements (15) pour recalculer la signature du message reçu à partir du contenu du message du programme et de la clé secrète précités, un dispositif de comparaison (16) dont la première entrée reçoit la signature (SG)

du message reçu et dont la seconde entrée reçoit la signature recalculée, un dispositif témoin (16) indiquant le résultat vrai ou différent de la comparaison précitée, l'entrée du dispositif témoin étant reliée à la sortie du dispositif de comparaison, caractérisé en ce que :

- l'émetteur comprend en outre un objet portatif (1b), dénommé carte nominative de signature, contenant au moins ledit programme (P) et ladite clé secrète (S),
- le récepteur comprend en outre un objet portatif (3b), dénommé carte de contrôle accessible à plusieurs personnes, contenant au moins ledit programme (P) et ladite clé secrète (S)".

IX. En ce qui concerne la brevetabilité des revendications indépendantes 1 et 4, selon la requête principale, les parties présentèrent les arguments suivants.

L'Appelante se référa, en particulier, aux passages suivants du document E1 :

- le paragraphe : "Digital signatures" (page 832 à 833),
- le paragraphe : "A reliable digital signature method" (page 835 à 836),
- le paragraphe : "Simplification of the proposed signature architecture" (page 836), et
- la partie finale du paragraphe : "Conclusions" (page 837, colonne de droite, lignes 7 à 24).

Elle fit remarquer que le procédé pour authentifier l'auteur d'un message signé, tel que divulgué par lesdits passages de E1, était une amélioration du procédé de M. O. Rabin, divulgué par D2, et affirma que le procédé pour authentifier l'auteur d'un message signé, tel que défini par la revendication 1, était substantiellement

anticipé par l'enseignement divulgué par E1, cet enseignement étant lu, le cas échéant, à la lumière de celui divulgué par D2.

L'Intimée contesta la pertinence de l'enseignement divulgué par E1, en faisant valoir que cette antériorité divulguait

- un procédé pour authentifier la signature de l'auteur d'un message signé envoyé par un appareil émetteur à un appareil récepteur, dans lequel l'appareil émetteur crée automatiquement une signature élaborée par un programme de calcul en fonction au moins du message et d'une clé secrète inconnue de l'émetteur du message ; la vérification de l'identité de l'auteur du message étant faite à la demande du destinataire en utilisant au moins le message et la clé secrète, c'est-à-dire

- un procédé pour authentifier la signature de l'auteur d'un message signé tel que défini dans le préambule de la revendication 1.

Elle fit aussi valoir que, contrairement à ce qui était prescrit par la revendication 1, dans E1

- la transmission du message devait se faire forcément et uniquement par une voie de transmission protégée, et non par une voie quelconque,

- la vérification de l'identité de l'auteur du message devait et pouvait être exécutée uniquement par un organisme dénommé "Network Registry", et non par le destinataire du message lui-même, lequel, selon E1, n'avait même pas la possibilité matérielle d'exécuter une telle vérification,

- ledit "Network Registry", dont il n'existait aucun équivalent ou analogue dans l'invention, devait être un organisme indépendant aussi bien de l'auteur que du destinataire du message, parce qu'il devait pouvoir exercer la fonction confidentielle d'un "notaire" et, le cas échéant, celle impartiale d'un "juge", et

- ledit "Network Registry" exécutait la vérification de l'identité de l'auteur du message en utilisant un algorithme inverse de celui qui avait été utilisé lors de l'élaboration de ladite signature, et non en recalculant automatiquement la signature du message à partir du dit message et en utilisant le même programme de calcul et la même clé secrète utilisés pour l'élaboration de la signature.

L'Intimée affirma, en conséquence, que l'originalité inventive du procédé et du dispositif selon l'invention était à voir dans les faits suivants :

- la transmission du message, ainsi que de sa signature calculée conformément au préambule des revendications 1 et 4, pouvait se faire par une voie de transmission quelconque, c'est-à-dire, non protégée,

- la vérification de l'identité de l'auteur du message pouvait être exécutée par le destinataire du message lui-même, lequel avait bien à sa disposition tous les moyens nécessaires à exécuter ladite vérification en recalculant la signature dudit message, mais au contraire, aucun moyen susceptible de lui permettre de prendre connaissance de ladite signature recalculée, parce que le système lui indiquait seulement et uniquement le résultat -égal ou différent- de la comparaison entre ladite signature recalculée et celle reçue avec le message, et

- il n'existait aucun équivalent ou analogue du "Network Registry", ce qui impliquait une simplification remarquable du système.

L'Intimée admit qu'aussi dans E1 le destinataire du message n'avait aucune possibilité de prendre connaissance de la signature recalculée, mais elle tint à souligner que cela était uniquement la conséquence du fait que, selon E1, ledit destinataire n'avait à sa disposition aucun des moyens nécessaires à exécuter, lui même, la vérification de la signature d'un message reçu et donc, à fortiori, aucun des moyens nécessaires à la recalculer ; ces moyens étant uniquement à la disposition du "Network Registry".

X. En ce qui concerne la brevetabilité des revendications indépendantes 1 et 4, selon la requête subsidiaire, les parties présentèrent les arguments suivants.

L'Appelante fit préalablement remarquer que ces revendications étaient identiques à celles maintenues par la Division d'opposition et rappela que déjà pendant la procédure d'opposition (v. le procès verbale de la procédure orale ayant eu lieu le 26 novembre 1991, page 1, 6ème alinéa) elle avait objecté que ces revendications ne satisfaisaient pas aux exigences des articles 123(2) et 123(3) de la CBE. Elle réaffirma cette objection, qu'elle motiva

- en se référant à la demande n° 82 401 752, sur laquelle se base le brevet contesté,
- en faisant valoir que ladite demande, telle que déposée, divulguait uniquement des objets portatifs (carte de signature et carte de contrôle) contenant un programme (P) de calcul de la signature (SG) d'un message (M), une clé secrète (S) et des circuits de traitement (6, 15) destinés à calculer

-respectivement recalculer- ladite signature (SG), conformément audit programme (P) et en faisant appel au moins au message (M) et à ladite clé secrète (S), c'est-à dire des cartes ayant une fonction active,

- en faisant remarquer que les revendications 1 et 4 définissaient lesdits objets portatifs (carte de signature et carte de contrôle) comme contenant uniquement ledit programme (P) et ladite clé secrète (S), mais non lesdits circuits de traitement (6, 15), c'est-à dire comme des cartes ayant uniquement une fonction passive, et
- en faisant valoir que ladite demande, telle que déposée, ne divulguait aucunement des objets portatifs, tels que définis par lesdites revendications 1 et 4.

En suite, toujours en se référant à ladite demande telle que déposée, l'Appelante fit remarquer que, conformément au procédé et au dispositif selon le brevet contesté et tels que définis par les revendications 1 et 4, les objets portatifs qui doivent être accouplés à l'appareil émetteur, respectivement récepteur, étaient des cartes ayant une fonction active -connues aussi sous les dénominations : "cartes intelligentes" ou "smart-cards"- et étaient censées exécuter les fonctions suivantes :

- mémoriser ledit programme (P) et ladite clé secrète (S) de telle façon que ni l'un ni l'autre soient accessibles de l'extérieur, et
- calculer -respectivement recalculer- ladite signature (SG), conformément audit programme (P) et en faisant appel au moins au message (M) et à ladite clé secrète (S).

Elle fit valoir que les étapes du procédé selon E1 et celles du procédé selon le brevet contesté étaient à tel point semblables, qu'il n'était pas possible de

concevoir, à fortiori de définir, une différence substantielle entre

- les fonctions qui, conformément au procédé selon E1, doivent être exécutées au niveau des appareils émetteur et récepteur, et
- les fonctions qui, conformément au procédé selon le brevet contesté, doivent être exécutées, au niveau des appareils émetteur et récepteur, par lesdits objets portatifs.

Elle fit aussi valoir que, à la date de priorité du brevet contesté, tout homme du métier était bien au courant des possibilités offertes par lesdites "smart-cards" et, plus en particulier, du fait qu'il était parfaitement possible de confier à de telles cartes l'exécution des fonctions prévues par le procédé selon E1, aussi bien que de celles qui, conformément au procédé selon le brevet contesté, doivent être exécutées, au niveau des appareils émetteur et récepteur, par lesdits objets portatifs.

En se référant au document E2 (page 2, ligne 22 à page 3, ligne 25 ; page 4, lignes 16 à 36), l'Appelante fit remarquer que ce document divulguait un système de transmission de messages chiffrés entre un appareil émetteur et un appareil récepteur, dans lequel ces deux appareils ne pouvaient fonctionner, si non à la condition que deux objets portatifs soient accouplées l'un à l'appareil émetteur et l'autre à l'appareil récepteur ; ces deux objets portatifs étant aussi du type "smart-cards" et destinés à exécuter des fonctions tout-à-fait analogues à celles qui doivent être exécutées par les objets portatifs selon le brevet contesté, à savoir :

- mémoriser un programme de calcul (p) et au moins une clé secrète (S) de telle façon que ni l'un ni l'autre soient accessibles de l'extérieur,

- calculer une clé de chiffrement (R1) -au niveau de l'appareil émetteur- et une clé de déchiffrement (R2) -au niveau de l'appareil récepteur- ; ces deux clés (R1, R2) étant les mêmes et étant calculées conformément audit programme (p) et en faisant appel au moins à un code d'identification (In), lié au contenu de l'information à transmettre, et à ladite clé secrète (S).

Tout en admettant que dans E2 il était question

- de chiffrer la totalité de l'information transmise, c'est-à-dire la totalité du message, et non uniquement la signature dudit message, et
- de calculer les deux clés de chiffrement (R1 = R2) en faisant appel uniquement à un code d'identification (In), lequel, tout étant lié au contenu de l'information à transmettre, ne représentait pas la totalité de ladite information -totalité du message-,

l'Appelante fit, néanmoins, valoir que, eu égard à l'analogie flagrante qui existe entre les fonctions qui sont exécutées par les objets portatifs selon E2 et celles prévues par le procédé selon E1 ou celles qui doivent être exécutées par les objets portatifs selon le brevet contesté, tout homme du métier, confronté avec le problème de déterminer la structure d'objets portatifs susceptibles d'exécuter les fonctions prévues par le procédé selon E1 ou celles devant être exécutées dans le brevet contesté, aurait immédiatement envisagé de confier l'exécution de ces fonctions à des "smart-cards" ayant une structure essentiellement identique à celle des objets portatifs selon E2, en aboutissant ainsi à

l'enseignement selon le brevet contesté, sans la nécessité d'exercer une activité inventive.

L'Intimée ne dénia point qu'à la date de priorité du brevet contesté, tout homme du métier était bien au courant des possibilités offertes par lesdites "smart-cards", ni que de telles cartes aient été utilisées, par exemple dans E2, pour exécuter des fonctions apparemment similaires à celles qui doivent être exécutées par les objets portatifs selon le brevet contesté.

Elle fit, toutefois, valoir que la similitude entre les fonctions exécutées par les "smart-cards" selon E2 et celles exécutées par les objets portatifs selon le brevet contesté se limitait

- à permettre aux porteurs desdites "smart-cards" de s'identifier auprès du système comme étant des personnes autorisées à utiliser ledit système, mais non comme une personne physique donnée, auteur du message transmis, et
- à mémoriser un programme de calcul (p) et au moins une clé secrète (S) de telle façon que ni l'un ni l'autre soient accessibles de l'extérieur.

Elle souligna que toutes les autres fonctions étaient totalement différentes et, en particulier, que dans E2

- il n'était absolument pas question de calculer la signature (SG) d'un message, conformément à un programme (P) et en faisant appel au moins au message (M) et à une clé secrète (S), et

- il était même tout-à-fait impossible de recalculer ladite signature (SG), conformément audit programme (P) et en faisant appel au moins au message (M) et à

ladite clé secrète (S), parce que, dans E2, la totalité du message était transmise en forme chiffrée et il venait donc a manquer, au niveau de l'appareil récepteur, l'un des éléments indispensables afin de pouvoir recalculer ladite signature (SG).

Elle fit, enfin, valoir que, si dans E2 les deux clés (R1) et (R2) étaient décrites comme étant les mêmes et comme étant des clés de "chiffrement", il n'était pas moins vrai qu'elles étaient utilisées pour chiffrer (R1), respectivement déchiffrer (R2), la totalité du message, tandis que la notion même d'un tel chiffrement et déchiffrement était complètement inconnue dans le brevet contesté.

Elle affirma, en conséquence, qu'un homme du métier n'aurait jamais envisagé de combiner l'enseignement divulgué par E1 avec celui divulgué par E2 afin de résoudre le problème posé dans le brevet contesté ; ce problème étant celui de permettre au destinataire d'un message signé, de vérifier, lui-même et directement, si la signature accompagnant ledit message est bien celle de la personne qui déclarait en être l'auteur, tout en interdisant au récepteur du message la possibilité de pouvoir prendre connaissance de la "valeur" de la signature recalculée ("valeur" = structure binaire).

XI. Avant que les débats ne soient clôturés et sur requête du Président de la Chambre, les parties formulèrent les requêtes suivantes.

L'Appelante demanda l'annulation de la décision contestée et la révocation du brevet européen n°0 077 238, dans sa totalité.

L'Intimée demanda le rejet du recours, et le maintien du brevet modifié, selon le premier jeu de revendications

(requête principale) ou selon le troisième jeu de revendication (requête subsidiaire), reçus le 18 mai 1993.

XII. Après la clôture des débats et le délibéré de la Chambre, le Président annonça la révocation du brevet contesté.

XIII. Après cette annonce de la part du Président de la Chambre, l'Intimée rappela qu'au cours de la procédure écrite elle avait avancé la requête qu'il lui soit permis de présenter de nouvelles revendications, "au cas où aucun de ces jeux de revendications ne seraient acceptables", et sollicita qu'une opportunité de présenter de nouvelles revendications lui soit accordée.

XIV. L'Appelante affirma qu'une telle requête, après que la présente décision avait déjà été annoncée, n'était pas recevable et demanda à la Chambre de rejeter cette requête tardive.

XV. Avant de délibérer sur ce point, la Chambre invita l'Intimée à spécifier la portée des nouvelles revendications qu'elle se proposait de présenter.

XVI. L'Intimée spécifia qu'elle se proposait de présenter

- une nouvelle revendication 1 (revendication indépendante de procédé) résultante de la fusion des revendications 1, 2 et 3 telles que délivrées, et

- une nouvelle revendication 2 (revendication indépendante de dispositif) résultante de la fusion des revendications 4, 5, 6 et 7, telles que délivrées ; les revendications 8, 9, 10 et 12, telles que délivrées, mais renumérotées 3, 4, 5 et 6 restant dépendantes de la revendication 2 (de dispositif).

XVII. L'Appelante affirma que les sujets des nouvelles revendications indépendantes, telles que spécifiées par l'Intimée, n'étaient pas davantage brevetables que ceux des revendications indépendantes selon les requêtes principale et subsidiaire car ils n'impliquaient pas davantage une activité inventive.

Au cas où la Chambre considérerait lesdites nouvelles revendications comme recevables, elle demanda que le brevet contesté soit néanmoins révoqué pour les motifs présentés aux égards des revendications indépendantes selon les requêtes principale et subsidiaire.

Elle demanda aussi, au cas où l'affaire serait renvoyée devant la Première Instance pour l'examen desdites nouvelles revendications, que les dépenses qui seraient impliquées par cette nouvelle étape de la procédure soient supportées par l'Intimée.

XVIII. Après délibéré de la Chambre, le Président annonça le rejet de la dernière requête de l'Intimée.

Motifs de la décision

1. Le recours répond aux conditions énoncées aux articles 106, 107 et 108, ainsi qu'à la règle 64 de la CBE ; il est donc recevable.

2. *Articles 123(2) et 123(3)*

La Chambre constate que les revendications indépendantes 1 et 4, aussi bien selon la requête principale que selon la requête subsidiaire, ne coïncident pas avec les revendications indépendantes 1 et 4, telles que délivrées.

En conséquence, la question si oui ou non toutes ces revendications satisfont aux exigences des articles 123 (2) et 123 (3), devrait être examinée au préalable, bien qu'une objection aux termes desdits articles n'ait été soulevée qu'aux égards des revendications 1 et 4 selon la requête subsidiaire.

La Chambre est toutefois de l'avis qu'un tel examen est indispensable seulement si les sujets desdites revendications 1 et 4, selon la requête principale ou selon la requête subsidiaire, devaient être considérés comme brevetables aux termes des article 52 (1), 54 et 56 de la CBE.

3. *Nouveauté*

3.1 Document D1

Cette antériorité divulgue un procédé et un dispositif pour authentifier la signature de l'auteur d'un message signé et transmis, sur une voie de transmission quelconque, par un appareil émetteur à un appareil récepteur, dans lesquels

- un objet portatif (4), devant être accouplé temporairement à l'appareil émetteur, crée automatiquement :
  - une signature (SG) élaborée par un programme de calcul (P2) en fonction du message (M), d'une clé secrète (J) inconnue de l'émetteur du message, et d'un code d'identification (In) lié à la nature des messages que le porteur de l'objet portatif (4) est habilité à transmettre, et associe ladite signature (SG) ainsi calculée audit message (M), et

- une clé de chiffrement (R1) élaborée par un programme de calcul (P1) en fonction d'une clé banale (E) préalablement transmise à l'appareil récepteur, d'une clé secrète (S) connue de l'émetteur et du destinataire du message, et dudit code d'identification (In), et utilise ladite clé de chiffrement (R1) ainsi élaborée pour chiffrer l'ensemble représenté par ladite signature (SG) associée audit message (M) ; ledit ensemble étant transmis à l'appareil récepteur en une forme ainsi chiffrée ;

- un objet portatif (5), devant être accouplé temporairement à l'appareil récepteur, crée automatiquement :
  - une clé de chiffrement (R2 = R1) élaborée par ledit programme de calcul (P1) en fonction de ladite clé banale (E) préalablement reçue, de ladite clé secrète (S), et dudit code d'identification (In), et utilise ladite clé de chiffrement (R2) ainsi élaborée pour déchiffrer l'ensemble représenté par ladite signature (SG) associée audit message (M) ; ledit message (M) résultant ainsi "en claire", tandis que sa signature (SG) reste sous la forme : "SG = P2 (M, J, In)", telle que élaborée par l'objet portatif (4) au niveau de l'appareil émetteur ;

- la vérification de l'identité de l'auteur du message étant faite, à la demande du destinataire, par un organisme indépendant aussi bien de l'auteur que du destinataire du message, lequel
  - exécute ladite vérification en utilisant ledit message (M) et ladite clé secrète (J), dont il est dépositaire, pour recalculer ladite signature (SG),

- compare la signature ainsi recalculée à celle qui était associée audit message, et
- communique au destinataire du message uniquement le résultat -égal ou différent- de ladite comparaison ; le résultat "égal" constituant la certification que la signature (SG) associée audit message (M) était bien celle de la personne qui prétendait en être l'auteur.

Lesdits objets portatifs (4) et (5) comportent tous les circuits de traitement nécessaires à l'exécution des élaborations et calculs indiqués ci-dessus. Ledit programme de calcul (P1), ledit code d'identification (In) et ladite clé secrète (S) sont enregistrés, de façon inaccessible de l'extérieur, dans l'un et dans l'autre desdits objets portatifs (4) et (5), tandis que, dans l'objet portatif (4) sont enregistrés, aussi de façon inaccessible de l'extérieur, uniquement ledit programme de calcul (P2) et ladite clé secrète (J).

Le procédé et le dispositif pour authentifier la signature de l'auteur d'un message signé, tels que définis par les revendications 1 et 4 selon l'une quelconque des requêtes de l'Intimée, sont nouveaux par rapport à ceux divulgués par D1 ; la nouveauté étant à voir dans les faits suivants :

- dans D1, la vérification de l'identité de l'auteur d'un message doit et peut être exécutée uniquement par un organisme indépendant aussi bien de l'auteur que du destinataire du message, et non par le destinataire du message lui-même, lequel, selon D1, n'a pas la possibilité matérielle d'exécuter une telle vérification, faute des moyens nécessaires, à savoir : le programme de calcul (P2) et la clé secrète (J), et

- dans D1, il est prévu d'exécuter un chiffrement -à l'émission- et un déchiffrement -à la réception- de l'ensemble représenté par la signature (SG) associée au message (M), au moyen des clés de chiffrement (R1 et R2) ; un tel chiffrement et déchiffrement étant complètement inconnus dans le brevet contesté.

3.2 Document E1

Le procédé pour authentifier l'auteur d'un message signé, divulgué par E1, est une amélioration du procédé de M. O. Rabin, divulgué par D2, auquel les auteurs de E1 font maintes fois référence tout au long de leur exposé, ce qui leur permet de ne mentionner explicitement certaines notions qui sont, par contre, explicitement mentionnées par D2.

La Chambre est, par conséquent, de l'avis que l'enseignement divulgué par E1 ne peut être correctement apprécié, si non en lisant E1 à la lumière de D2, c'est-à-dire en considérant que l'enseignement divulgué par E1 contient, par implication, aussi toutes les notions qui sont explicitement mentionnées par D2 et qui ne sont pas explicitement rejetées par E1 comme n'étant pas applicables au procédé selon ce dernier.

Lu de la façon indiquée ci-dessus, E1 divulgue un procédé pour authentifier l'auteur d'un message signé envoyé par un appareil émetteur à un appareil récepteur, dans lequel l'appareil émetteur crée automatiquement une signature élaborée par un programme de calcul en fonction au moins du message et d'une clé secrète inconnue de l'émetteur du message (v. page 836, colonne de gauche, lignes 28 à 34), la vérification de l'identité de l'auteur étant faite à la demande du destinataire en utilisant au moins le message et la clé secrète, lequel, pour vérifier l'authenticité de la

signature d'un message reçu par l'appareil récepteur, comporte les étapes suivantes :

- on recalcule automatiquement la signature du message reçu à partir d'au moins le même programme de calcul et de la même clé secrète inconnue de l'émetteur du message précités,
- on compare automatiquement la signature du message reçu et la signature recalculée au niveau de l'appareil récepteur (v. page 836, colonne de gauche, lignes 35 à 42), et
- on indique au récepteur du message, seulement le résultat égal ou différent de la comparaison précédente, tout en interdisant au récepteur du message la possibilité de pouvoir prendre connaissance de la "valeur" (structure binaire) de la signature recalculée (v. E1 : page 832, colonne de droite, point 1 : "Unforgeability", où il est fait écho à D2 : page 156 à page 157, paragraphe I).

Bien que E1 ne divulgue pas un dispositif détaillé destiné à réaliser le procédé résumé ci-dessus, la Chambre ne peut pas agréer les affirmations de l'Intimée, selon lesquelles, dans E1,

- la transmission du message devait se faire forcément et uniquement par une voie de transmission protégée, et non par une voie quelconque, et
- la vérification de l'identité de l'auteur du message devait et pouvait être exécutée uniquement par un organisme dénommé "Network Registry", et non par le destinataire du message lui-même, lequel, selon E1, n'avait même pas la possibilité matérielle d'exécuter une telle vérification.

Dans E1, en effet, il est bien envisagé

- que chaque machine -appareil émetteur et récepteur- puisse travailler comme un unique domaine protégé, ce qui dispense de l'utilisation d'une voie de transmission protégée (v. page 837, colonne de droite, lignes 16 à 19), et
- que puissent exister des communications directes entre les appareils émetteur et récepteur, sans l'intervention du "Network Registry" (v. page 836, colonne de gauche, lignes 41 à 45 et page 837, colonne de droite, lignes 9 à 11, "point-to-point communications"), ce qui implique bien la nécessité de permettre, au destinataire du message, d'exécuter lui-même la vérification de l'identité de l'auteur dudit message. De plus, la notion d'une telle vérification doit être considérée comme implicite dans E1, car elle est explicitement mentionnée par D2 (page 159 à page 160, paragraphes V et VI).

La Chambre ne peut pas davantage agréer l'affirmation de l'Intimée, selon laquelle, dans E1, le "Network Registry" aurait exécuté la vérification de l'identité de l'auteur du message en utilisant un algorithme inverse de celui qui avait été utilisé lors de l'élaboration de ladite signature, et non en recalculant automatiquement la signature du message à partir du dit message et en utilisant le même programme de calcul et la même clé secrète utilisés pour l'élaboration de la signature.

Dans E1, en effet, il est bien divulgué que

- la signature ("signature block") est élaborée par un programme de calcul en fonction au moins du message et d'une clé secrète inconnue de l'émetteur du message et que l'organe ayant élaboré ledit "signature block" retient, dans sa mémoire,

uniquement la clé secrète utilisée (v. page 836, colonne de gauche, lignes 28 à 34), et
- la vérification de la signature ("signature block") est faite uniquement sur la base dudit "signature block" et du message (v. page 836, colonne de gauche, lignes 35 à 38), ce qui implique que l'organe devant exécuter la vérification de la signature n'a à sa disposition aucun autre élément, si non ceux qui permettent de recalculer ledit "signature block".

Il semble, donc, légitime de considérer que les étapes principales du procédé pour authentifier l'auteur d'un message signé, tel que défini par la revendication 1 selon la requête principale, soient anticipées par l'enseignement divulgué par E1, cet enseignement étant lu à la lumière de celui divulgué par D2.

Le procédé et le dispositif pour authentifier la signature de l'auteur d'un message signé, tels que définis par les revendications 1 et 4 selon la requête subsidiaire, sont, par contre, nouveaux par rapport à ceux divulgués par E1 ; la nouveauté étant à voir dans le fait que ce document ne divulgue pas, tout au moins expressis verbis, un dispositif détaillé pour la mise en oeuvre du procédé qu'il propose, dans lequel

- lors de l'élaboration de ladite signature, un objet portatif (1b) dénommé carte nominative de signature, contenant au moins ledit programme (P) et ladite clé secrète (S) doit être accouplé à l'appareil émetteur, et
- lors de l'authentification de ladite signature, un objet portatif (3b), dénommé carte de contrôle accessible à plusieurs personnes, contenant au moins ledit programme (P) et ladite clé secrète (S) doit être accouplé à l'appareil récepteur.

3.3 Document E2 divulgue (page 2, ligne 22 à page 3, ligne 25 ; page 4, lignes 16 à 36) un système de transmission de messages chiffrés entre un appareil émetteur et un appareil récepteur, dans lequel ces deux appareils ne peuvent fonctionner, si non à la condition que deux objets portatifs soient accouplées l'un à l'appareil émetteur et l'autre à l'appareil récepteur ; ces deux objets portatifs étant du type "smart-cards" et destinés à exécuter les fonctions suivantes :

- mémoriser un programme de calcul (p) et au moins une clé secrète (S) de telle façon que ni l'un ni l'autre soient accessibles de l'extérieur,
- calculer une clé de chiffrement (R1) -au niveau de l'appareil émetteur- et une clé de chiffrement (R2) -au niveau de l'appareil récepteur- ; ces deux clés (R1, R2) étant les mêmes et étant calculées conformément audit programme (p) et en faisant appel au moins à un code d'identification (In), lié au contenu de l'information à transmettre, et à ladite clé secrète (S).

Le procédé et le dispositif pour authentifier la signature de l'auteur d'un message signé, tels que définis par les revendications 1 et 4 selon la requête subsidiaire, sont nouveaux par rapport à ceux divulgués par E2 ; la nouveauté étant à voir dans le fait que, dans ce document

- il n'est pas question de calculer la signature (SG) d'un message, conformément à un programme (P) et en faisant appel au moins au message (M) et à une clé secrète (S),
- il est même tout-à-fait impossible de recalculer ladite signature (SG), conformément audit programme (P) et en faisant appel au moins au message (M) et à ladite clé secrète (S), parce que, dans E2, la

totalité du message est transmise en forme chiffrée et il vient donc à manquer, au niveau de l'appareil récepteur, l'un des éléments indispensables afin de pouvoir recalculer ladite signature (SG),

- il est prévu d'exécuter un chiffrement, à l'émission, et un déchiffrement, à la réception, de l'ensemble représenté par la signature (SG) associée au message (M), au moyen des clés de chiffrement (R1 et R2) ; un tel chiffrement et déchiffrement étant complètement inconnus dans le brevet contesté.

4. *Problème et solution*

L'Intimée a affirmé que le problème technique, dont le brevet contesté se proposait de trouver une solution, était celui de permettre au destinataire d'un message signé, de vérifier, lui-même et directement, si la signature accompagnant ledit message était bien celle de la personne qui déclarait en être l'auteur, tout en interdisant audit récepteur du message la possibilité de pouvoir prendre connaissance de la "valeur" de la signature recalculée.

4.1 Eu égard aux enseignements respectivement divulgués par D1 et par E1 -qui représentent les états de la technique les plus proches, la Chambre est d'avis qu'un homme du métier aurait bien envisagé de se poser le problème indiqué ci-dessus, ayant pris en considération uniquement l'enseignement divulgué par D1, lequel, en effet, n'envisage même pas de permettre au destinataire d'un message signé, de vérifier, lui-même et directement, l'authenticité de la signature dudit message et donc, à fortiori, n'envisage pas les conditions et les précautions à prendre, afin que la possibilité d'une telle vérification soit donnée au destinataire d'un message signé.

4.2 La Chambre est, par contre, d'avis qu'un homme du métier, ayant pris en considération l'enseignement divulgué par E1, n'aurait même pas envisagé de se poser un tel problème, parce que E1

- envisage bien de permettre au destinataire d'un message signé, de vérifier, lui-même et directement, l'authenticité de la signature dudit message (v. E1 : page 836, colonne de gauche, lignes 41 à 45 et page 837, colonne de droite, lignes 9 à 11, "point-to-point communications", où il est fait écho à D2 : page 159 à page 160, paragraphes V et VI), et, en conséquence,

- envisage aussi les conditions et les précautions à prendre afin que la possibilité d'une telle vérification soit donnée au destinataire d'un message signé (v. E1 : page 832, colonne de droite, point 1 : "Unforgeability", où il est fait écho à D2 : page 156 à page 157, paragraphe I).

4.3 Eu égard aux considérations qui précèdent, la Chambre est d'avis que le problème, que le brevet contesté se proposait effectivement de résoudre, était celui de définir un dispositif détaillé pour la mise en oeuvre du procédé selon E1 et comportant tous les moyens matériels nécessaires à assurer la vérification des conditions et des précautions à prendre, afin que la possibilité de vérifier l'authenticité de la signature d'un message signé puisse être effectivement donnée au destinataire dudit message, lui-même ; ces moyens devant être tels que le système de transmission de messages signés puisse fonctionner en l'absence d'un organisme du type "Network Registry", mais devant être, néanmoins, tels à ne pas donner, au destinataire d'un premier message, la possibilité

- de reproduire la signature dudit premier message reçu,
- d'associer cette signature reproduite à un deuxième message, et
- de faire ainsi croire à une troisième personne que l'auteur dudit deuxième message est la même personne qui a envoyé ledit premier message.

4.4 La solution de ce problème, telle que divulguée par le brevet contesté, est représentée par les caractéristiques suivantes :

a) lors de l'élaboration de ladite signature, un objet portatif (1b), dénommé carte nominative de signature, contenant au moins ledit programme (P) et ladite clé secrète (S), est accouplé à l'appareil émetteur,

b) lors de l'authentification de ladite signature, un objet portatif (3b), dénommé carte de contrôle accessible à plusieurs personnes, contenant au moins ledit programme (P) et ladite clé secrète (S), est accouplé à l'appareil récepteur,

c) lesdits objets portatifs (1b et 3b) étant arrangés de façon telle à interdire à la personne réceptrice du message la possibilité de pouvoir prendre connaissance de la valeur de la signature recalculée, et.

d) ledit programme (P) et ladite clé secrète (S) étant enregistrés dans lesdits objets portatifs (1b et 3b) par un organisme chargé de leur production et initialisation, lors de cette production et initialisation, ce qui permet de réaliser un système de transmission de messages signés pouvant fonctionner en l'absence de voies

de transmission protégées reliant un organisme du type "Network Registry" aux appareils émetteur et récepteur.

Il convient, toutefois, de souligner que la solution revendiquée par les revendications 1 et 4 selon la requête subsidiaire est représentée uniquement par les caractéristiques a), b) et c) ci-dessus.

5. *Activité inventive*

Il convient de rappeler que E1

- ne divulgue pas une définition complète d'un dispositif détaillé pour la mise en oeuvre du procédé qu'il propose et comportant tous les moyens matériels nécessaires à assurer la vérification des conditions et des précautions à prendre, afin que la possibilité de vérifier l'authenticité de la signature d'un message signé puisse être effectivement donnée au destinataire dudit message, lui-même (point 4.3), mais
- envisage bien lesdites conditions et précautions à prendre afin que la possibilité d'une telle vérification soit donnée au destinataire d'un message signé (v. E1 : page 832, colonne de droite, point 1 : "Unforgeability", où il est fait écho à D2 : page 156 à page 157, paragraphe I) (point 4.2), et, de ce fait,
- suggère déjà, par implication, une définition, tout au moins fonctionnelle, d'un dispositif pour la mise en oeuvre du procédé qu'il propose et des moyens matériels devant être compris par ledit dispositif ; ces moyens devant être tels qu'ils puissent mettre en oeuvre les notions qui sont intrinsèques dans le premier et essentiel principe, sur lequel se base le

procédé de M. O. Rabin, divulgué justement par D2 (page 156 à page 157, paragraphe I).

A ce propos il convient de rappeler que ce principe comporte les notions suivantes :

- ayant indiqué avec M un message et avec $o_p(M)$ la signature qu'une personne P a apposé sur ledit message M, cette signature $o_p(M)$ doit avoir la propriété (a) : uniquement la personne P doit être en mesure de produire des messages signés, formés par une quelconque couple M et $o_p(M)$,
- cette propriété (a) est bien plus restrictive que la simple présomption que seulement la personne P puisse signer un message M donné, parce que cette propriété (a) entraîne que la signature $o_p(M)$ est une caractéristique non seulement de la personne P, mais aussi de la totalité du message M, et

- si une autre personne ("adversary"), ayant reçu un message signé donné N, formé par le couple N et $o_p(N)$, pouvait trouver un autre message M différent de N, mais tel qu'il soit $o_p(M) = o_p(N)$, alors cette autre personne serait en mesure de produire un message signé M, formé par le couple M et $o_p(M)$, dont la personne P ne serait quand même pas l'auteur, ce qui serait en contradiction avec la propriété (a).

5.1 En ce qui concerne l'activité inventive pouvant être impliquée par la position du problème technique à résoudre, tel que défini dans le point 4.3 précédent, il convient de se référer au chapitre : "USER AUTHENTICATION", aux pages 836 et 837 de E1, dans lequel ce dernier analyse et cherche à définir les caractéristiques d'un élément -appelé "box"- qui doit être compris dans le dispositif pour la mise en oeuvre

du procédé qu'il divulgue ; cet élément devant être tel que, si d'une part

- il assure que la possibilité de vérifier l'authenticité de la signature d'un message signé puisse être effectivement donnée au destinataire, lui-même, dudit message, d'autre part
- il ne doit pas donner, au destinataire d'un premier message, la possibilité de reproduire la signature dudit premier message reçu, d'associer cette signature reproduite à un deuxième message, et de faire ainsi croire à une troisième personne que l'auteur dudit deuxième message est la même personne qui a envoyé ledit premier message.

5.2 Eu égard à ce qui précède, la Chambre est d'avis qu'aucune activité inventive ne peut être considérée comme impliquée par la pure et simple position du problème technique à résoudre, tel que défini dans le point 4.3 précédent.

5.3 En ce qui concerne l'activité inventive pouvant être impliquée par la solution dudit problème, telle que divulguée par le brevet contesté (point 4.4), il convient de se référer, encore une fois, au chapitre : "USER AUTHENTICATION", aux pages 836 et 837 de E1, dans lequel ce dernier envisage que le "box", en addition aux caractéristiques fonctionnelles indiquées dans le point 5.1 précédent, doit aussi avoir au moins les fonctions de

- permettre à son utilisateur attitré de s'identifier d'une manière absolument certaine auprès du système, plus précisément auprès d'une unité locale -terminal d'ordinateur- constituant l'appareil émetteur qu'il va utiliser pour envoyer un message (v. page 836, colonne de droite, lignes 37 à 45), et
- contenir, dans sa mémoire, au moins la clé secrète, devant être utilisée pour le calcul de la signature

d'un message, de manière telle que cette clé secrète ne puisse pas être lue de l'extérieur, ce qui rende le "box" complètement inutilisable pour toute personne autre que son utilisateur attitré (v. page 836, colonne de droite, ligne 52 à page 837, colonne de gauche, ligne 10).

Parmi les formes possibles de réalisation matérielle dudit "box", E1 envisage celle d'une carte et, compte tenu que cette carte doit comporter au moins toutes les caractéristiques fonctionnelles indiquées ci-dessus, il est légitime de conclure que la carte envisagée par E1 est du type "smart-card".

Enfin, compte tenu des conclusions mentionnées par E1 (v. page 837, colonne de gauche, ligne 44 à colonne de droite, ligne 21), il est aussi légitime de considérer que E1

- suggère, tout au moins, d'enfermer, dans des "smart-cards" devant être accouplées temporairement aux terminaux du système de transmission, tous les éléments -software et hardware- qui sont nécessaires à la mise en oeuvre du procédé qu'il divulgue, et
- considère que l'utilisation de "smart-cards" ainsi structurées est bien susceptible de permettre des communications directes entre émetteur et récepteur, lesquelles peuvent avoir lieu sur des voies non protégées et essentiellement en l'absence d'un organisme du type "Network Registry", dont le rôle indispensable se réduirait à celui du producteur et distributeur desdites "smart-cards" ainsi structurées.

5.4 Compte tenu des suggestions et considérations qu'un homme du métier se devait de considérer comme implicites dans E1 (point 5.3 ci-dessus) et de l'analogie qui existe entre les fonctions qui sont exécutées par les

objets portatifs selon E2 et celles prévues par le procédé selon E1 (points 3.2 et 3.3), la Chambre se doit de partager l'avis de l'Appelante (point X du "Résumé"), selon lequel, eu égard à l'analogie flagrante qui existe entre les fonctions qui sont exécutées par les objets portatifs selon E2 et celles prévues par le procédé selon E1 ou celles qui doivent être exécutées par les objets portatifs selon le brevet contesté, un homme du métier, confronté avec le problème de déterminer la structure d'objets portatifs susceptibles d'exécuter les fonctions prévues par le procédé selon E1 ou celles devant être exécutées dans le brevet contesté, aurait immédiatement envisagé de confier l'exécution de ces fonctions à des "smart-cards" ayant une structure essentiellement identique à celle des objets portatifs selon E2, en aboutissant ainsi à la solution, telle que divulguée par le brevet contesté (point 4.4), du problème technique à résoudre par ce dernier (point 4.3), sans la nécessité d'exercer une activité inventive.

5.5 La Chambre est, en conséquence, de l'avis que

- les sujets des revendications indépendantes 1 et 4, selon la requête subsidiaire, lesquelles mentionnent uniquement les caractéristiques identifiées avec les références a), b) et c) dans le point 4.4 précédent, et
- les sujets des revendications indépendantes 1 et 4, selon la requête principale, lesquelles ne mentionnent pas du tout les caractéristiques identifiées avec les références a), b) et c) dans le point 4.4 précédent, n'impliquent, *a fortiori*, pas une activité inventive aux termes de l'article 56 de la CBE.

6. *Conclusions*

Les revendications indépendantes 1 et 4, selon l'une quelconque des requêtes de l'Intimée, ne sont donc pas brevetables aux termes des articles 52(1) et 56 de la CBE.

Les requêtes principale et subsidiaire doivent être refusées pour ce motif, ce qui entraîne que le brevet doit être révoqué.

7. La requête de l'Intimée, qu'il lui soit permis de présenter des nouvelles revendications (v. points XII à XIV du "Résumé"), appelle le considérations suivantes.

Conformément à des principes généraux du droit de procédure, aucune requête ne peut être recevable après qu'une décision a été annoncée, dans une procédure écrite ou à la fin d'une procédure orale (v. décision T 598/88, du 7 août 1989).

Avant la procédure orale, l'Intimée avait avancé, par écrit, la requête qu'il lui soit permis de présenter de nouvelles revendications, au cas où aucune des requêtes principale ou subsidiaire ne serait considérée comme acceptable.

Au cours de la procédure orale, cette dernière requête écrite ne fut pas réitérée, si non après que la décision avait déjà été annoncée oralement, suite au délibéré de la Chambre.

La requête de l'Intimée, de prendre en considération de nouvelles revendications n'est donc pas recevable.

La Chambre considère, néanmoins, opportun de mentionner que, même si l'Intimée avait présenté sa requête au

cours de la procédure orale et avant que la décision ne fut annoncée, cette requête n'aurait été quand même pas recevable pour les raisons suivantes.

Conformément à la jurisprudence établie des Chambres de Recours, toute modification d'une demande ou d'un brevet, devant être prise en considération au cours d'une procédure orale, doit être déposée bien à l'avance (v. décision T 153/85, Journal Officiel OEB, 1988, 1).

En outre, afin d'être recevable, toute modification tardive doit satisfaire aux critères suivants :

- elle doit y avoir une justification claire aussi bien pour la modification que pour son dépôt tardif, et la modification doit être telle à remédier un défaut constaté dans les revendications d'origine (v. décisions T 95/83, Journal Officiel OEB, 1995, 75 ; et T 33/91 du 19 décembre 1991),

- la modification tardive ne doit pas entraîner un retard appréciable de la procédure (v. T 166/86, Journal Officiel OEB, 1977, 372), et

- elle doit représenter une tentative, faite en bonne foi, dans le but de surmonter une objection soulevée au cours de la procédure (v. décision T 38/89 du 21 août 1990).

Compte tenu
- que la brevetabilité des revendications selon la nouvelle requête ne pouvait pas être jugée sans un examen nécessitant un temps considérable,
- qu'aucune justification pour son dépôt tardif ne fut donnée (l'Intimée fut informée bien longtemps avant la procédure orale des objections soulevées contre la

brevetabilité des requêtes qu'elle avait avancées, aussi bien par l'Appelante que par la Chambre), et

- qu'il n'a pas été établi que la requête représentait une tentative, faite en bonne foi, dans le but de surmonter une objection soulevée au cours de la procédure,

aucun des critères indiqués ci-dessus n'a été satisfait.

Elle est, en outre, jurisprudence établie des Chambres de Recours que toute modification tardive d'une demande ou d'un brevet peut être refusée, lorsque la procédure est substantiellement complète (v. décision T 406/86, Journal Officiel OEB, 1989, 302).

Pour chacune de ces raisons, donc, ladite requête reste non recevable.

La Chambre considère, en conséquence, qu'elle n'a aucune nécessité de statuer

- ni sur la brevetabilité des nouvelles revendications que l'Intimée se proposait de présenter (point XVI du "Résumé),
- ni sur les requêtes de l'Appelante (point XVII du "Résumé).

Dispositif

Par ces motifs, il est statué comme suit :

1. La décision contestée est annulée.

2. Les requêtes principale et subsidiaire de l'Intimée sont refusées.

3. Le brevet est révoqué

4. La requête de l'Intimée, qu'il lui soit donné l'opportunité de présenter des nouvelles revendications est rejetée comme non recevable.

Le Greffier : Le Président :

M. Kiehl P.K.J. van den Berg