TRIBUNAL DE GRANDE INSTANCE DE PARIS
JUGEMENT rendu le 14 avril 2016

3ème chambre 1ère section
N° RG : 14/11998

DEMANDERESSE
Société Koninklijke KPN N.V.
Maanplein 55, 2516 CK. "s-Gravenhage
LA HAYE (PAYS-BAS)
représentée par Maître Sabine AGE de la SCP SCP D'AVOCATS VERON & ASSOCIES, avocats au barreau de PARIS, avocats postulant, vestiaire #P0024 et par Maîtres Thomas B et Caroline L, avocats plaidants

DÉFENDERESSE
S.A.INGENICO GROUP anciennement dénommée COMPAGNIE INDUSTRIELLE ET FINANCIERE D'INGENIERIE INGENICO
[...]
75015 PARIS
représentée par Maître François hERPE de la SELARL C.V.S., avocat au barreau de PARIS, vestiaire #P0098

COMPOSITION DU TRIBUNAL
Marie-Christine C Vice-Présidente
Julien RICHAUD, Juge
Aurélie JIMENEZ. Juge
assistés de Léoncia B. Greffier

DÉBATS
À l'audience du 15 mars 2016 tenue publiquement devant Julien RICHAUD et Aurélie JIMENEZ, juges rapporteurs, qui, sans opposition des avocats, ont tenu seuls l'audience, et, après avoir entendu les conseils des parties, en ont rendu compte au Tribunal, conformément aux dispositions de l'article 786 du Code de Procédure Civile

JUGEMENT
Prononcé publiquement par mise à disposition au greffe
Contradictoirement
en premier ressort

EXPOSE DU LITIGE
La société de droit néerlandais KONINKLIJKE KPN NV, qui se présente comme le plus gros opérateur néerlandais de téléphonie fixe et mobile et comme un important fournisseur d'accès internet et de télévision en ligne aux Pays-Bas, a pour activité principale la fourniture de services et de solutions informatiques dans le domaine des technologies de l'information et de la communication.

Elle est titulaire des droits de propriété intellectuelle sur le brevet européen n° 0 873 554 visant la France intitulé « méthode pour débiter un moyen de paiement électronique » dont la demande a été déposée le 14 novembre 1996 sous priorité d'une demande de brevet néerlandais n° 1 001 659 du 15 novembre 1995 et publiée le 28 octobre 1998 et qui a été délivré le 20 septembre 2000.

Ce brevet est maintenu en vigueur par le paiement régulier des redevances annuelles dans neuf États membres dont la France.

La SA INGENICO GROUP, anciennement dénommée COMPAGNIE INDUSTRIELLE ET FINANCIERE D'INGENIERIE INGENICO, est la société mère du groupe INGENICO et est spécialisée dans l'offre et la vente ou à la location en France et à l'étranger de multiples solutions de paiement sécurisées et intégrées et notamment de terminaux de paiement fixes ou mobiles acceptant plus de 250 moyens de paiement avec ou sans contact de la carte à puce.

La société de droit néerlandais KONINKLIJKE KPN NV explique que la norme internationale EMV, conçue en 1994 par les trois fabricants de cartes de crédit Europay. Mastercard et Visa pour servir de standard aux cartes de paiement à puce et aux terminaux de paiement et modifiée en juin 2007, juin 2008 et novembre 2011 sous des versions 4.1.4.2 et 4.3. définit un procédé d'authentification des transactions par la méthode CDA qui met en œuvre le procédé de paiement enseigné et protégé par le brevet européen n° 0 873 554. Soutenant que la SA INGENICO GROUP fabrique, conçoit, détient, offre et vend des dispositifs de paiement pour carte à puce qu'elle présente comme étant homologués selon cette norme, elle en déduit que l'offre et la vente des terminaux de paiement conformes à la norme EMV dans ses versions 4.1,4.2 et 4.3 constituent des actes de contrefaçon de son brevet.

Par courrier du 18 février 2013, la société de droit néerlandais KONINKLIJKE KPN NV a mis la SA INGENICO GROUP en demeure de cesser ces actes et lui a proposé la conclusion d'une licence de son brevet.

Les échanges de courriers ultérieurs n'ayant pas permis le règlement amiable du litige naissant, la société de droit néerlandais KONINKLIJKE KPN NV a été autorisée, par ordonnance du 9 juillet 2014 rendue par le délégataire du président du tribunal de grande instance de Paris, à faire pratiquer une saisie-contrefaçon au siège social de la SA INGENICO GROUP. Les opérations de saisie-contrefaçon se sont déroulées le 16 juillet 2014.

C'est dans ces circonstances que la société de droit néerlandais KONINKLIJKE KPN NV a, par acte d'huissier du 14 août 2014, assigné la SA INGENICO GROUP devant le tribunal de grande instance de PARIS en contrefaçon de la partie française de son brevet européen.

Dans ses dernières conclusions notifiées par la voie électronique le 6 janvier 2016 auxquelles il sera renvoyé pour un exposé de ses moyens conformément à l'article 455 du code de procédure civile, **la société de droit néerlandais KONINKLIJKE KPN NV demande au tribunal,** sous le bénéfice de l'exécution provisoire et au visa des dispositions des articles L 613-4, L 615-1, L 615-7, L 615-7-1 du code de la propriété intellectuelle :

de débouter la société Ingenico de sa demande reconventionnelle en nullité du brevet européen n° 0 873 554 de la société KPN ;

de dire et juger que la société Ingenico se rend coupable de contrefaçon des revendications n° 1, 2, 3 et 6 de la partie française du brevet européen n° 0 873 554 de la société KPN en offrant et commercialisant des terminaux de paiement mettant en œuvre le procédé de paiement CDA de la norme EMV ;

de condamner la société Ingenico à cesser les actes de contrefaçon sous astreinte non comminatoire de 5 000 euros par infraction constatée dans le délai de huit jours suivant la signification du jugement à intervenir, étant précisé que l'offre de livraison ou la livraison de tout terminal de paiement constitueront une infraction distincte ;

de condamner la société Ingenico à réparer le préjudice causé à la société KPN, le montant des dommages et intérêts devant être fixé par le tribunal après expertise et condamner dès à présent la société Ingenico à payer à la société KPN une provision sur dommages et intérêts d'un montant de 500 000 euros ;

de désigner tel expert qu'il plaira au tribunal afin de fournir au tribunal toutes les informations nécessaires à l'évaluation du préjudice subi par la société KPN et plus particulièrement avec pour mission :

de déterminer les quantités totales de terminaux de paiement livrés en France par les sociétés Ingenico, sur la période non prescrite, jusqu'à la date de dépôt du rapport ;

de déterminer le chiffre d'affaires correspondant réalisé par toutes les sociétés du groupe Ingenico, en précisant le rôle éventuel de chacune de ces sociétés dans les actes jugés contrefaisants :

de rechercher le taux de redevance indemnitaire qui aurait été dû si la société Ingenico avait demandé une licence du brevet ou accepté celle proposée par la société KPN :

d'évaluer distinctement le préjudice moral subi par la société KPN et les bénéfices réalisés par la société Ingenico du fait de la contrefaçon :

de dire que les opérations d'expertise porteront sur tous les actes de contrefaçon commis jusqu'à la date de dépôt du rapport ;

d'ordonner la publication du jugement, par extraits, dans trois revues ou journaux au choix de la société KPN et aux frais de la société Ingenico, celle-ci devant contribuer auxdites publications pour un montant de 1 000 euros par publication :

de condamner la société Ingenico à payer à la société KPN la somme de 200 000 euros au titre de l'article 700 du code de procédure civile :

de condamner la société Ingenico aux entiers dépens de l'instance et accorder au cabinet Véron & Associés le bénéfice de l'article 699 du code de procédure civile.

En réplique, dans ses dernières écritures notifiées par la voie électronique le 9 février 2016 auxquelles il sera renvoyé pour un exposé de ses moyens conformément à l'article 455 du code de procédure civile, la SA INGENICO GROUP demande au tribunal, au visa des dispositions des articles L 614-12, L 613-4 et I. 615-1 et suivants du code de la propriété intellectuelle, de la Convention sur le brevet européen (CBE) et notamment l'article 138 § 1 a) et c), de l'article 232 du code de procédure civile :
à titre principal :
de dire et juger que les revendications 1, 2, 3 et 6 de la partie française du brevet EP n° 0 873 554 sont nulles pour extension de l'objet, dans la mesure où l'objet du brevet EP n°0 873 554 s'étend au-delà du contenu de la demande telle qu'elle a été déposée: de dire et juger que les revendications 1, 2, 3 et 6 de la partie française du brevet EP n° 0 873 554 sont nulles pour défaut de nouveauté :
de dire et juger que les revendications 1, 2, 3 et 6 de la partie française du brevet EP n° 0 873 554 sont nulles pour défaut d'activité inventive:
en conséquence :
de déclarer nulles les revendications 1, 2, 3 et 6 de la partie française du brevet EP n° 0 873 554 :
d'ordonner la transmission du jugement à intervenir à l'INPI aux fins d'inscription au Registre National des Brevets :
à titre subsidiaire, de dire et juger que la société Ingenico Group n'a commis aucun acte de contrefaçon des revendications 1 à 3 et 6 du brevet EP n° 0 873 554;
en tout état de cause :
de débouter la société Koninklijke KPN N.V. de l'intégralité de ses demandes, fins et conclusions à l'encontre de la société Ingenico Group:
de condamner la société Koninklijke KPN N.V. à payer à la société Ingenico Group la somme de 240 000 euros au titre de l'article 700 du code de procédure civile :
de condamner la société Koninklijke KPN N.V. aux entiers dépens de la présente instance, que la SELARL CVS, prise en la personne de Maître François H, pourra recouvrer, conformément aux dispositions de l'article 699 du code de procédure civile.

L'ordonnance de clôture était rendue le 23 février 2016. Les parties ayant régulièrement constitué avocat, le présent jugement, rendu en premier ressort, sera contradictoire en application de l'article 467 du code de procédure civile.

MOTIFS DU JUGEMENT

1°) Sur la validité de la partie française du brevet européen n° 0 873 554

La société de droit néerlandais KONINKLIJKL KPN NV est titulaire des droits de propriété intellectuelle sur la partie française du (le) brevet européen n° 0 873 554 (visant la France) intitulé « méthode pour débiter un moyen de paiement électronique » dont la demande a été déposée le 14 novembre 1996 sous priorité d'une demande de brevet néerlandais n° 1 001 659 du 15 novembre 1995 et publiée le 28 octobre 1998 et qui a été délivré le 20 septembre 2000.

Conformément aux dispositions combinées de l'article 7 de l'Acte portant révision de la Convention sur la délivrance de brevets européens du 29 novembre 2000 entré en vigueur le 13 décembre 2007 et de l'article 1er la Décision du Conseil d'administration du 28 juin 2001 : les articles 14 (3) à (6), 51, 52, 53, 54 (3) et (4), 61, 67, 68, 69 et le protocole interprétatif de l'article 69, ainsi que les articles 70, 86, 88, 90, 92, 93, 94, 97, 98, 106, 108, 110, 115, 117, 119, 120, 123, 124, 127, 128, 129, 133, 135, 137 et 141 sont applicables aux demandes de brevet européen pendantes ainsi qu'aux brevets européens déjà délivrés à la date de leur entrée en vigueur. Toutefois, l'article 54 (4) du texte de la convention en vigueur avant cette date continue de s'appliquer à ces demandes et brevets, les articles 65, 99, 101, 103, 104, 105, 105bis à quater, et 138 sont applicables aux brevets européens déjà délivrés à la date de leur entrée en vigueur ainsi qu'aux brevets européens délivrés pour des demandes de brevet européen pendantes à cette date.

En outre en vertu de la Décision du Conseil d'administration du 12 décembre 2002 adoptant le règlement d'exécution de la CBE 2000 et de l'article 2 de la Décision du Conseil d'administration du 7 décembre 2006 modifiant le règlement d'exécution de la CBE 2000, le règlement d'exécution de la CBE 2000 s'applique à l'ensemble des demandes de brevet européen, des brevets européens et des décisions des instances de l'Office européen des brevets ainsi qu'aux demandes internationales, dans la mesure où ils sont soumis aux dispositions de la CBE 2000.

Dans ce cadre, conformément aux articles 2 « Brevet européen » et 3 « Portée territoriale » de la Convention de Munich du 5 octobre 1973, le brevet européen peut être demandé pour un ou plusieurs des États contractants et a, dans chacun des États contractants pour lesquels il est délivré, les mêmes effets et est soumis au même régime qu'un brevet national délivré dans cet État, sauf si la convention en dispose autrement.

Et, en application de l'article 52§1 « Inventions brevetables » de la Convention, les brevets européens sont délivrés pour toute invention dans tous les domaines technologiques, à condition qu'elle soit nouvelle, qu'elle implique une activité inventive et qu'elle soit susceptible d'application industrielle

a) **Sur la portée du brevet**

Moyens des parties

La société de droit néerlandais KONINKLIJKE KPN NV explique que la protection conférée par un brevet, déterminée par la teneur des revendications lue à la lumière de la description et des dessins, dépend d'une part de la catégorie à laquelle appartient la revendication (revendication de produit, revendication de procédé ou d'utilisation en vue d'obtenir un produit ou un effet) et d'autre part des caractéristiques techniques ou fonctionnelles indiquées dans les revendications et en déduit que, dès lors qu'une revendication d'utilisation définit l'utilisation d'une chose particulière comme une utilisation en vue d'obtenir un effet et non un produit, elle ne constitue pas une revendication de procédé dont l'objet s'étend au produit obtenu directement par le procédé mais protège uniquement l'utilisation de la chose visée pour la fonction indiquée, avec tous les éléments structurels mentionnés.

Dans ce cadre, elle expose que son brevet a pour objet un procédé de paiement entre une carte à puce et un terminal de paiement et entend répondre au problème technique de la sécurisation des transactions selon un protocole de paiement protégé garantissant l'authenticité de la carte et l'intégrité de la transaction. Elle précise que le procédé repose sur l'existence d'une part de deux étapes pendant chacune desquelles le poste de paiement transmet une information à la carte qui répond par l'envoi d'un code d'authentification, préférentiellement crypté, déterminé sur la base de l'information adressée par le poste de paiement et sur la base d'autres informations, les étapes intermédiaires étant facultatives et indifférentes à la sécurisation de la transaction, et d'autre part d'un lien entre les premier et deuxième codes d'authentification, ce lien étant obtenu en utilisant une donnée provenant de la première étape d'échanges pour produire le deuxième code d'authentification. Elle indique en outre que la description ne contient aucune limitation sur la façon dont la fonction F produit la première valeur finale (Y 1) qui peut porter sur tout élément entrant dans le calcul de la fonction et couvrir des fonctions de cryptographie symétrique ou asymétrique.

Elle explique enfin que le mode de réalisation donné dans la description concernant les cartes électroniques à prépaiement ne limite pas la portée de l'invention qui se rapporte à tout mode de paiement par carte à puce telle une carte à puce bancaire, le transfert du solde pouvant être omis ou remplacé par un accusé de réception de la transaction ou par une authentification de carte. Elle précise à cet égard que tant les revendications que la description et les dessins, en particulier la figure 1 qui montre une carte à puce utilisée pour procéder à un règlement dans un commerce et reliée à la banque du porteur de la carte et à celle du commerçant, révèlent que l'expression « moyen de paiement électronique » couvre tout type de carte à puce et non uniquement une carte prépayée rechargeable, cette expression, visible dans les spécifications EMV dès 1994, désignant

d'ailleurs en 1996 (une erreur matérielle affectant à l'évidence ses écritures qui visent l'année 2006) de manière générale, comme les termes « carte à puce » ou « carte intelligente », tout type de carte de paiement dont les cartes bancaires. Elle ajoute que les modifications apportées à la revendication n° 1 du brevet pendant la procédure de délivrance, destinées à améliorer la clarté de la revendication et non à la distinguer de l'art antérieur, ne peuvent justifier sa lecture restrictive.

En réplique, la SA INGENICO GROUP expose que le brevet concerne d'une part un procédé d'exécution, de façon protégée, d'une transaction de débit entre une carte à unités à débiter et un terminal, ce procédé mettant obligatoirement en œuvre un protocole spécifique en six étapes imposant une liaison ou un chaînage entre les codes d'authentification envoyés successivement par le moyen de paiement au poste de paiement, et d'autre part un produit consistant uniquement en un moyen de paiement mettant en œuvre ce procédé et non en un poste de paiement ou terminal.

Elle indique que l'invention entend résoudre le problème de l'indépendance entre les codes d'authentification, qui ne prévient pas les risques de fraude par substitution du moyen de paiement, par l'utilisation d'un résidu cryptographique produit lors de l'étape initiale pour chaîner les étapes entre elles et par le stockage sur celui-ci de ce résidu destiné à être réutilisé dans l'étape ultérieure, le tout assurant que le moyen de paiement n'a pas été changé et que le solde à débiter est bien celui du même moyen de paiement. Elle en déduit que, le terminal et la carte effectuant les mêmes calculs et disposant ainsi de la même clef secrète de chiffrement, la fonction F emploie un algorithme de cryptographie symétrique, les codes dénommés MAC 1 en Step I, et MAC 2 en Step III étant d'ailleurs produits par des algorithmes symétriques de chiffrement, et que le brevet couvre un système fermé de dialogue sécurisé entre une carte et un poste de paiement sans communication ni échanges ou étapes avec d'autres systèmes, dispositifs, serveurs ou institutions. Elle ajoute que, le dialogue entre le moyen de paiement et le poste de paiement de type «challenge/réponse » étant compris dans l'art antérieur, la partie caractérisante de la revendication 1 de procédé réside uniquement dans la liaison ou le chaînage des codes d'authentification entre eux.

Elle expose enfin que le procédé s'applique uniquement aux cartes contenant un solde d'unités de valeur à débiter voire à créditer mais non aux cartes bancaires ainsi que le révèlent le titre, le contenu, le contexte et les modes de réalisation préférés de l'invention et la procédure de délivrance, la figure 1, dont la description est sommaire et ne définit aucun moyen permettant d'informer au moins une des deux banques de façon sécurisée de ce qu'elle doit exécuter cette transaction, ne contredisant pas cette analyse. Elle précise à ce titre que le terme de «transaction » ne peut que signifier « débit » ou « crédit » d'un montant stocké dans un moyen de paiement et que les données S1 et S2 sont des données représentatives du solde de ce

dernier. Elle en déduit que le brevet couvre la sécurisation du solde stocké sur une carte à unités à débiter.

Appréciation du tribunal

En vertu de l'article 164 « Règlement d'exécution et protocole » de la Convention, le règlement d'exécution et le protocole interprétatif de l'article 69 font partie intégrante de la présente convention, les dispositions de la Convention prévalant en cas de divergence.

En application des règles 42 « Contenu de la description » et 43 « Forme et contenu des revendications » du Règlement d'exécution de la Convention (antérieurement 27 et 29). le brevet comprend :
une description précisant notamment le domaine technique auquel se rapporte l'invention, indiquant l'état de la technique antérieure et exposant l'invention, telle qu'elle est caractérisée dans les revendications, avec au moins un mode de réalisation, des revendications en nombre raisonnable définissant, en indiquant les caractéristiques techniques de l'invention, l'objet de la demande pour lequel la protection est recherchée et contenant en particulier un préambule mentionnant la désignation de l'objet de l'invention et les caractéristiques techniques qui sont nécessaires à la définition de l'objet revendiqué mais qui, combinées entre elles, l'ont partie de l'état de la technique ainsi qu'une partie caractérisante introduite par l'expression "caractérisé en" ou "caractérisé par" exposant les caractéristiques techniques pour lesquelles, en liaison avec les caractéristiques indiquées en préambule, la protection est recherchée.

Ainsi, la structure de la revendication est essentielle à la détermination de l'assiette du droit et du champ de la protection offerte par le titre. Le préambule de la revendication expose l'état de la technique tandis que la partie caractérisante, introduite par les termes « caractérisé en »ou «par », présente les éléments constitutifs de l'invention, les moyens nouveaux et inventifs pris clans leur forme et leur fonction qui s'appliquent à l'objet compris dans l'art antérieur et sont exclusivement protégés. La partie caractérisante n'est prise « en liaison » avec le préambule que parce que celui-ci est le support de celle-là et que les moyens pour lesquels la protection est revendiquée et accordée s'appliquent au produit décrit dans le préambule. Ce lien, comme l'interprétation faite à la lumière de la description et des dessins, n'a pas pour effet d'étendre la protection à des éléments insusceptibles de monopole puisque compris dans l'état de la technique mais d'identifier l'objet concret des moyens constituant l'invention. L'atteinte au droit exclusif est d'ailleurs caractérisée non par la reproduction d'éléments du préambule mais par celle des moyens revendiqués dans la partie caractérisante.

Conformément à l'article 69 « Étendue de la protection » de la Convention, l'étendue de la protection conférée par le brevet européen ou par la demande de brevet européen est déterminée par les

revendications, qui au sens de l'article 84 « revendications » définissent l'objet de la protection demandée et doivent être claires et concises, se fonder sur la description et être interprétées à la lumière de la description et des dessins. Pour la période allant jusqu'à la délivrance du brevet européen, l'étendue de la protection conférée par la demande de brevet européen est déterminée par les revendications contenues dans la demande telle que publiée. Toutefois, le brevet européen tel que délivré ou tel que modifié au cours de la procédure d'opposition, de limitation ou de nullité détermine rétroactivement la protection conférée par la demande, pour autant que cette protection ne soit pas étendue.

Et, le Protocole interprétatif de l'article 69 de la Convention dispose que :
« Article premier - Principes généraux : l'article 69 ne doit pas être interprété comme signifiant que l'étendue de la protection conférée par le brevet européen est déterminée au sens étroit et littéral du texte des revendications et que la description et les dessins servent uniquement à dissiper les ambiguïtés que pourraient receler les revendications. Il ne doit pas davantage être interprété comme signifiant que les revendications servent uniquement de ligne directrice et que la protection s'étend également à ce que, de l'avis d'un homme du métier ayant examiné la description et les dessins, le titulaire du brevet a entendu protéger. L'article 69 doit, par contre, être interprété comme définissant entre ces extrêmes une position qui assure à la fois une protection équitable au titulaire du brevet et un degré raisonnable de sécurité juridique aux tiers.
Article 2 - Équivalents : pour la détermination de l'étendue de la protection conférée par le brevet européen, il est dûment tenu compte de tout élément équivalent à un élément indiqué dans les revendications ».

L'invention porte sur « une méthode pour débiter un moyen de paiement électronique» et, «en particulier, bien que non exclusivement. [... sur] un procédé destiné à débiter de façon protégée des cartes de paiement électronique à prépaiement ("cartes à prépaiement") telles qu'elles sont utilisées, par exemple, pour des cabines téléphoniques ».

Il est rappelé dans la partie descriptive du brevet qu'il est nécessaire que l'échange de données entre un moyen de paiement, qui comprend généralement un solde (crédit) représentant une valeur monétaire, et un poste de paiement se fasse selon un procédé protégé (protocole de paiement) destiné à garantir la corrélation entre le débit et le crédit de l'un et de l'autre. Il est indiqué que l'on connaissait déjà, en particulier dans la demande de brevet EP 0 637 004 antérieurement déposée par la demanderesse, des procédés de paiement comprenant 3 étapes permettant de déterminer le solde du moyen de paiement, de le réduire puis de récupérer le solde résultant, la différence entre le premier et le dernier montant permettant de définir

les montants débité et à créditer, et dans lesquels la prévention de la fraude était réalisée par l'utilisation, dans la première et dans la troisième étapes, d'un nombre aléatoire généré par le poste de paiement puis transféré au moyen de paiement qui produit un code d'authentification pouvant comprendre une forme élaborée telle qu'une forme cryptographique notamment du nombre aléatoire et du solde. Si un tel procédé est efficace puisque le nombre aléatoire est différent pour chaque transaction et évite Limitation de la transaction par reproduction, il ne fait pas obstacle, les deux codes d'authentification étant indépendants, à la séparation de la première étape des deux autres en cas de communication avec d'autres postes de paiement et à la réalisation d'une transaction complète en apparence mais sans débit du moyen de paiement. L'utilisation de l'identité du module de sécurité du poste de paiement pour garantir qu'un échange de données a lieu entre la carte et seulement un terminal enseignée par le brevet US 5 495 098 rend complexe la protection de l'échange de données entre le module de sécurité, le poste et la carte, et nécessite d'amples calculs cryptographiques.

Pour répondre à ces inconvénients, le brevet propose :
un procédé qui offre un degré encore plus grand de protection des transactions de débit et garantit le crédit d'un seul poste de paiement pendant une transaction en liant les codes d'authentification par l'utilisation lors d'une étape d'interrogation d'une valeur initiale obtenue à l'occasion de l'étape d'interrogation initiale, un produit constitué par un moyen de paiement pour l'application du procédé.

Le brevet se compose à cette fin de 16 revendications dont deux revendications principales 1 de procédé et 10 de produit, les revendications 2 à 9 étant des revendications de procédé dépendantes de la première et les revendications 11 à 16 étant des revendications de produit dépendantes de la 10. Seules les revendications 1 ,2, 3 et 6 sont opposées par la société de droit néerlandais KONINKLIJKE KPN NV. Toutefois, l'analyse de la portée du brevet s'opérant en considération de toutes les revendications dépendantes ainsi que de la description et des dessins, leur contenu sera rappelé. Les revendications à 1 à 9 sont ainsi rédigées :

revendication 1 : « Procédé d'exécution de façon protégée d'une transaction en utilisant un moyen (11) de paiement électronique et un poste (12) de paiement, le procédé comprenant : une étape initiale (I), dans laquelle :
le poste 12 de paiement transfère une première valeur aléatoire (R1) au moyen (11) de paiement ;
le moyen (11) de paiement, en réponse à ladite première valeur aléatoire (R1) transfère un premier code (MAC 1) d'authentification au poste (12) de paiement, lequel code d'authentification est déterminé sur la base d'au moins une première valeur (Ql) de départ, de la première valeur aléatoire (RI) et de premières données (SI) de transaction du moyen (11) de paiement, en utilisant un traitement (F)

prédéterminé, le traitement produisant en outre une première valeur finale (YI) :
une étape ultérieure (III), dans laquelle :
le poste (12) de paiement transfère une seconde valeur aléatoire (R2) au moyen (11) de paiement :
le moyen (11) de paiement transfère un second code (MAC2) d'authentification au poste (12) de paiement, lequel code d'authentification est déterminé sur la base d'au moins une seconde valeur (Q2) de départ, de la seconde valeur aléatoire (R2) et de secondes données (S2) de transaction du moyen (11) de paiement, en utilisant ledit traitement (F), la seconde valeur (Q2) de départ étant basée sur la première valeur finale (YI) » ;
revendication 2 : « Procédé selon la revendication 1, dans lequel la seconde valeur (02) de départ est identique à la première valeur Finale (Y1)»:
revendication 3 : « Procédé scion la revendication 1 ou 2, dans lequel on détermine aussi un code (par exemple. MACI) d'authentification sur la base d'une clé (K) et/ou d'un code d'identification »
revendication 4: «Procédé selon la revendication 1, 2 ou 3, comprenant une étape intermédiaire optionnelle (II) effectuée entre l'étape initiale (1) et des étapes ultérieures (III). dans lequel : le poste (12) de paiement transfère une instruction (D) au moyen (11) de paiement, et le solde du moyen (11) de paiement est modifié sur la base de l'instruction (D) » :
revendication 5 : « Procédé selon l'une quelconque des revendications précédentes, dans lequel la première valeur aléatoire (R1) et la seconde valeur aléatoire (R2) sont identiques, la sous-étape du poste (12) de paiement transférant la seconde valeur aléatoire (R2) au moyen (11) de paiement étant supprimée » :
revendication 6 : « Procédé selon l'une quelconque des revendications précédentes, dans lequel le traitement (F) implique une fonction de cryptographie » :
revendication 7 : « Procédé selon l'une quelconque des revendications précédentes, comprenant en outre une quatrième étape (IV), dans laquelle : le poste (12) de paiement enregistre la différence (S1 - S2) entre les soldes des première et troisième étapes » ;
revendication 8 : « Procédé selon l'une quelconque des revendications précédentes, dans lequel la troisième étape (III) s'effectue de manière répétée » ;
revendication 9 : « Procédé selon l'une quelconque des revendications précédentes, dans lequel le poste (12) de paiement comprend un module destiné à enregistrer des données de manière protégée ».

Le brevet comporte en outre 5 Figures, la première « montrant| schématiquement un système de paiement auquel peut s'appliquer l'invention », les Figures 2 à 4 illustrant le procédé et une variante de son mode de réalisation et la Figure 5 concernant le circuit intégré du moyen de paiement.

La nature des inconvénients prêtés à l'art antérieur et la formulation de la solution qu'entend apporter la société de droit néerlandais KONINKLIJKL KPN NV (page 4. lignes 1 à 4) révèlent que le problème technique auquel l'invention répond est celui de la sécurisation des transactions, le lien de dépendance entre les étapes d'interrogation et les codes d'authentification étant la réponse qui lui est donnée.

Le sens des revendications 2, 3 et 6 n'est pas en débat, seul celui de la revendication 1 opposant les parties. À cet égard, la procédure de délivrance et les variations éventuelles entre la demande et le titre délivré sont sans pertinence dans le cadre de l'analyse de la portée du brevet qui s'opère exclusivement en considération du second d'une part car celui-ci constitue le siège de la protection à compter de sa publication au sens de l'article 64 de la Convention, la protection conférée par l'article 67 à la demande de brevet n'étant que provisoire, et d'autre part car la sécurité juridique explicitement évoquée par le protocole interprétatif de l'article 69 commande que les tiers puissent déterminer l'étendue de la protection à la seule lecture du titre sans avoir à se livrer à l'interprétation hasardeuse de l'intention du déposant à l'aune des modifications intervenues depuis la demande.

La structure de la revendication 1 n'est pas conforme au Règlement d'exécution faute de comporter une partie caractérisante clairement annoncée. Il est constant que le dialogue entre le terminal et la carte ainsi que la production par celle-ci d'un code d'authentification intégrant une valeur aléatoire transmise par celui-là aux étapes initiale et ultérieure relèvent de l'état de la technique tel qu'il est décrit dans la description (page 2, lignes 12 à 31 et page 3. lignes 1 à 6) ainsi que dans le brevet EP 0 637 004 auquel elle se réfère expressément. Ainsi, le seul élément présenté comme nouveau consiste dans le lien de dépendance entre les deux codes d'authentification permise par l'utilisation pour générer le second de la valeur finale produite lors de l'étape initiale. La description confirme cette analyse en précisant (page 5, ligne 2 à 18) que « le procédé selon l'invention est donc caractérisé en ce que la seconde valeur de départ est basée sur la première finale » et que, « en basant la seconde valeur de départ sur la première valeur finale, c'est-à-dire sur l'état du traitement après la fin du premier code d'authentification, on obtient un couplage direct entre l'étape initiale (la première) et les étapes restantes », le processus pouvant être répété pour d'autres étapes supplémentaires (page 5. ligne 21). La figure 3 est également en ce sens quand elle montre que Y1 (première valeur finale) est égale à Q2 (seconde valeur de départ) conformément à la revendication 2 qui est un mode de réalisation particulier de la revendication 1 qui envisage une seconde valeur de départ « basée sur » la première valeur finale. C'est d'ailleurs ce lien de dépendance qui, seul, répond au problème de sécurisation posé par la description et qui empêche d'« interrompre le procédé ou d'échanger des données avec d'autres postes de paiement sans en être averti » (page 5, ligne 6 à 9, puis page 9, lignes 24 à 31 qui rappelle les inconvénients de l'art antérieur sur ce plan et

lignes 26 à 31 pour un raisonnement a contrario). À ce titre, le fait que le mode de réalisation revendiqué comporte 3 phases d'échanges qui peuvent être découpées en 6 étapes de transfert de données et d'instructions est indifférent car la présentation en 2 étapes est expressément adoptée par le brevet qui précise que l'étape intermédiaire (instruction de débit) est facultative et non essentielle à l'invention (description page 8, ligne 13 et revendication 4), le nombre total des étapes peut être augmenté (page 5. ligne 21 et page IL ligne 15) et le couplage direct entre l'étape initiale et une étape ultérieure étant l'élément essentiel de l'invention.

Et, la première valeur finale Y1 est générée parallèlement au premier code d'authentification puisque la description (page 4, ligne 22) et la revendication 1 utilisent la locution adverbiale « en outre » évocatrice d'un supplément ou « de plus » (page 11, ligne 4 : « La fonction F produit un code MAC1 d'authentification. De plus, l'état (le « résidu ») de la fonction F est sauvegardé en tant que première valeur finale Y1 »). Le dessin 2 confirme cette analyse en figurant 2 flèches distinctes, l'une associée au MAC1 et l'autre à Y1 et Q2. La valeur finale n'est ainsi pas préexistante à l'exécution du traitement dont elle est, comme le code d'authentification dont elle se distingue, le fruit. La description le confirme en expliquant (page 11, lignes 12 à 17) que, dans l'hypothèse où un troisième code d'authentification serait exigé, la seconde valeur finale, générée « en plus » du MAC2, « est l'état de la fonction F après traitement ».

Ainsi, la protection conférée par la revendication 1 porte sur un procédé de sécurisation d'une transaction lors d'un dialogue entre un moyen de paiement et un terminal de paiement par lequel la fonction de la carte génère sur la base d'une valeur aléatoire transmise par le terminal, outre un premier code d'authentification, une valeur qui sera réutilisée pour produire le second code d'authentification dans une étape ultérieure.

La fonction de la carte ou traitement n'est pas définie dans la revendication 1 et n'est caractérisée dans la revendication 6 qu'en ce qu'elle implique une fonction de cryptographie. La description évoque une fonction F «qui peut être une fonction de cryptographie [...] comme une fonction de DES (« de cryptage standard de données ») ou une fonction combinatoire relativement simple [...] ou une fonction de « hachage » ». Ainsi, il importe peu que l'homme du métier puisse ou non comprendre, par la référence à l'utilisation des sigles MAC et de la notion de résidu cryptographique ou par le fait que le terminal et la carte partagent la même clé de chiffrement, que la fonction de cryptage est nécessairement symétrique puisque celle-ci n'est pas revendiquée en tant que telle, l'invention portant sur le lien de dépendance entre les opérations successives d'authentification par la réutilisation d'une valeur finale produite lors de la phase précédente comme valeur initiale d'une phase suivante et non sur la manière dont sont générées ces valeurs et dont la protection n'est pas recherchée.

En revanche, tant la revendication 1 que la description et les figures 2 à 4 révèlent que le dialogue entre la carte et le terminal est fermé : aucune entité tierce n'intervient dans les échanges successifs. Seule la figure 1, qui « montre schématiquement un système de paiement auquel peut s'appliquer l'invention », mentionne la présence de banques.

Toutefois, outre le fait qu'un « système » est visé tandis que les figures 2 et 3, essentielles dans la description de la partie caractérisante de la revendication 1, désignent le « procédé » lui-même ce qui implique que ce dessin doive être considéré comme expliquant le lien de dépendance entre les phases PD1 (échanges carte/terminal) et PD2 (échanges entre banques) ainsi que le confirme la description (page 7, lignes 14 à 16 : « entre les institutions [...] un règlement a eu lieu par l'échange de données PD2 de paiement qui s'obtiennent à partir des données PD1 de paiement »), celle-ci n'est pas expliquée et le lien en pointillés entre la carte ou le terminal et la banque n'est pas défini. L'association évoquée entre la carte et la banque, comme celle existant entre le terminal et la banque, n'est pas compréhensible, les seuls échanges décrits étant ceux entre la carte et le terminal puis entre les établissements bancaires qui interviennent respectivement durant et après la transaction (page 7, lignes 10 à 15). Et, la formule « pendant une transaction il n'y a pas fondamentalement de communication entre le poste de paiement et l'institution de paiement (ce que l'on appelle système hors ligne) » doit s'entendre comme signifiant l'absence totale d'échange entre la carte ou le terminal et la banque non seulement car la précision faite entre parenthèses l'implique par définition mais car cette phrase annonce le rappel des risques d'abus précisément générés par ce défaut de communication (page 7, lignes 16 à 21). Dès lors, la figure 1 ne peut servir de fondement à la définition de l'objet auquel s'applique le procédé.

À cet égard, que le procédé soit destiné à obtenir un effet et non un produit n'empêche pas que l'analyse de la portée de la revendication le caractérisant soit déterminée en considération de l'objet auquel il s'applique. Or, le caractère strictement clos du dialogue entre la carte et le terminal implique par nature que les données de transaction visées dans la revendication 1 et symbolisées sur les figures 2 et 3 par S1 et S2 pour données chiffrées des soldes 1 et 2 (page 13, ligne 16) soient stockées dans le moyen de paiement, aucune interrogation d'un tiers sur l'état du solde n'étant prévue. Et, si la description est floue sur la nature du « moyen de paiement électronique » visé dans la revendication 1 et qui lui-même générique et trop imprécis au regard de la variété des produits qu'il recouvre (la description évoquant « non exclusivement » sous cette expression entendue dans « son sens large » des cartes prépayées, revalorisâmes et intelligentes ainsi que des moyens de paiement «autre qu'une carte» ou comprenant un portefeuille électronique), elle consacre tous ses développements, à l'exception de son ouverture finale au « crédit d'un moyen de paiement » (page 16, ligne 18), au débit d'une carte à puce (titre, contexte, résumé et modes de réalisations préférés).

Systématiquement, l'opération à sécuriser par le procédé porte sur la diminution, ou plus accessoirement sur l'augmentation, du solde des unités d'un moyen de paiement qui, en l'absence de tout dialogue avec un tiers susceptible de transmettre des données sur son état, est nécessairement contenu dans la carte elle-même. Le remplacement du transfert de solde de carte par un accusé de réception de diminution ou une authentification de carte dans l'hypothèse d'une répétition des transferts de solde (page 8, lignes 30 et 31 et page 9, lignes 1 à 7) ne contredit pas cette analyse, l'étape finale consistant malgré ce et nécessairement dans la détermination de la différence entre le premier et le dernier solde qui est enregistrée dans le terminal et l'opération supposant au moins un transfert de solde dont seule la répétition n'est pas présentée comme nécessaire (page 8, lignes 29 et 30). La revendication 7 porte d'ailleurs spécifiquement sur cette étape. Ainsi, le seul moyen de paiement envisagé dans la revendication 1, comme d'ailleurs dans les revendications de produit, est une carte comprenant un solde d'unités de valeur à débiter ou à créditer et non une carte bancaire, le simple fait que celle-ci soit également un moyen de paiement et soit désignée sous cette appellation générique dans les spécifications EMV étant sans pertinence, et les données de transaction transférées au terminal se limitent, codes d'authentification exceptés, aux soldes de la carte. En conséquence, la protection du procédé n'est pas étendue à la sécurisation des transactions par cartes bancaires qui suppose un dialogue ouvert et plus complexe.

L'examen de la procédure de délivrance et des variations entre la demande et le titre délivré n'ajoute rien à l'analyse de la portée du brevet ainsi opérée.

Les parties s'accordent pour définir l'homme du métier, à l'aune des connaissances et des capacités techniques duquel doivent s'apprécier tant l'accessibilité de l'antériorité destructrice de nouveauté que l'activité inventive qui conditionne la validité de l'enregistrement du brevet, est défini comme un cryptologue, qui est un ingénieur en informatique disposant d'un diplôme d'études supérieures, également mathématicien de formation, qui étudie et conçoit les méthodes de chiffrement.

b) Sur l'extension de l'objet du brevet au-delà du contenu de la demande

Moyens des parties

La SA INGENICO GROUP soutient que les modifications principales réalisées dans le texte et les revendications du brevet délivré ont consisté à supprimer l'étape optionnelle « Step II », à remplacer les expressions « payment means data » (« données du moyens de paiement») par « transaction data » (« données de transaction »), «balance » (« solde ») ou « the current balance » (« le solde actuel ») par « transaction data » (« données de transaction ») et à supprimer la référence SI ou S2 lorsqu'il n'était manifestement pas possible de

supprimer cette caractéristique « balance » (« solde »). Elle ajoute que la revendication 1 du brevet européen délivré correspond à une combinaison de la revendication indépendante 1 et de la revendication indépendante 5 de la demande de brevet telle que déposée,

Elle explique que, si le tribunal retient une acception large du terme «données de transaction », celle-ci ne trouve aucun support dans la demande et modifie la portée du brevet au-delà du contenu de la demande. Elle précise ainsi que les termes « transaction data » n'étaient visés dans la demande que pour désigner des données stockées par le terminal de paiement et non des données de transaction de la carte transférées à la station de paiement, les revendications 1 ou 5 usant de l'expression « payment means data » et les données du moyen de paiement n'étant pas des données de transaction de façon générale mais se résumant aux soldes S1 et S2 et aux codes d'authentification MAC1 et MAC2. Elle en déduit que, par cette modification, une caractéristique limitative présente dans la demande de brevet a été remplacée par une caractéristique non limitative de portée bien plus large puisque les données de transaction ne contiennent plus spécifiquement le code d'authentification et peuvent comprendre, par exemple, un horodatage ou la devise de la transaction.

En réplique, la société de droit néerlandais KONINKLIJKE KPN NV expose que l'examen du grief d'extension de l'objet du brevet suppose de comparer l'objet revendiqué, c'est-à-dire l'invention définie dans les revendications, avec le contenu de la demande telle que déposée, c'est-à-dire l'ensemble de la demande de brevet incluant la description, les revendications et les dessins. Elle en déduit que, faute pour la SA INGENICO GROUP qui se contente de comparer les revendications de démontrer que l'invention couverte par la revendication 1 du brevet délivré ne se trouve pas explicitement ou implicitement dans la description de la demande telle que déposée, sa demande doit être rejetée. Subsidiairement, elle précise que la demande enseigne clairement et expressément le procédé d'exécution conforme à celui couvert par la revendication 1 du brevet tel que délivré et que l'utilisation de l'expression « données de transaction du moyen de paiement » dans la revendication 1 du brevet délivré ne saurait constituer une extension de l'objet du brevet dès lors que le grief d'extension de son objet du brevet ne peut reposer sur le seul motif que la revendication ne contiendrait pas, mot à mot, des expressions figurant dans la demande qui utilise de surcroît l'expression « données de transaction » pour désigner les données échangées entre la carte et le terminal (page 7, lignes 1 à 6 de la traduction française). Elle en déduit que l'homme du métier comprend de ce passage et plus généralement du reste de la description que le poste de paiement contient une mémoire intégrée ou un module distinct contenant les données de transaction, que le moyen de paiement communique avec cette mémoire intégrée ou ce module distinct pour lui communiquer des données de transaction par l'intermédiaire du terminal de paiement, que les données de

transaction de la mémoire intégrée ou du module distinct du poste de paiement proviennent du moyen de paiement et constituent donc les « données de transaction du moyen de paiement » évoquées à la revendication n° 1 et que « les données de transaction » englobent les valeurs de solde de carte ou d'identification de la carte.

Appréciation du tribunal

En vertu de l'article L 614-12 du code de la propriété intellectuelle, la nullité du brevet européen est prononcée en ce qui concerne la France par décision de justice pour l'un quelconque des motifs visés à l'article 138, paragraphe 1, de la Convention de Munich. Si les motifs de nullité n'affectent le brevet qu'en partie, la nullité est prononcée sous la forme d'une limitation correspondante des revendications.

Et, conformément à l'article 138§lc de la Convention, le brevet européen ne peut être déclaré nul, avec effet pour un État contractant, que si l'objet du brevet européen s'étend au-delà du contenu de la demande telle qu'elle a été déposée ou, lorsque le brevet a été délivré sur la base d'une demande divisionnaire ou d'une nouvelle demande déposée en vertu de l'article 61, si l'objet du brevet s'étend au-delà du contenu de la demande antérieure telle qu'elle a été déposée.

La SA INGENICO GROUP livre une argumentation contradictoire en retenant au soutien de sa demande en nullité une définition de la notion de la transaction qu'elle combat pour déterminer la portée du brevet (page 29 de ses écritures : « le terme de « transaction » utilisé dans la revendication 1 ne peut que signifier « débit » ou « crédit » d'un montant stocké dans un moyen de paiement » et « l'interprétation élargie que tente d'en faire KPN, en suggérant que la « transaction » pourrait concerner tout échange de données entre une carte et un terminal, en particulier en vue de l'authentification de cette carte, relève d'une interprétation a posteriori tout à fait inappropriée et inacceptable »). Elle annonce d'ailleurs son raisonnement en en conditionnant la pertinence à l'adoption par le tribunal d'une acception large dans l'analyse de la portée du brevet. Or, il est désormais acquis que les termes de « données de transaction » du brevet tel que délivré ne couvrent, concernant le moyen de paiement et codes d'authentification exceptés, que les soldes, les termes « données du moyen de paiement » et « données de transaction » apparaissant ainsi équivalents comme l'avait suggéré l'examinateur dans son avis du 15 décembre 1997 qui soulignait le défaut de clarté des premiers. Ainsi, le moyen de nullité opposé par la SA INGENICO GROUP est sans objet.

En outre, la demande comprend dans sa description (traduction page 7, lignes 1 à 6) une référence aux données de transaction. S'il est exact qu'elle vise alors les données stockées dans la station de paiement dotée d'un stockage séparé ou d'un module intégré, cette précision intervient immédiatement après la mention de communication entre la carte et le terminal. Il est ainsi certain que les

données stockées sont également, pour partie au moins, celles qui ont été transférées par la carte au terminal.

En conséquence, la demande de nullité de la SA INGENICO GROUP sera rejetée à ce titre.

c) Sur la nouveauté

En vertu de l'article 54 « Nouveauté » de la Convention :
1) Une invention est considérée comme nouvelle si elle n'est pas comprise dans l'état de la technique.
2) L'état de la technique est constitué par tout ce qui a été rendu accessible au public avant la date de dépôt de la demande de brevet européen par une description écrite ou orale, un usage ou tout autre moyen.
3) Est également considéré comme compris dans l'état de la technique le contenu de demandes de brevet européen telles qu'elles ont été déposées, qui ont une date de dépôt antérieure à celle mentionnée au paragraphe 2 et qui n'ont été publiées qu'à cette date ou à une date postérieure.

Et, conformément à l'article 55 « Divulgations non opposables » de la Convention :
1) Pour l'application de l'article 54, une divulgation de l'invention n'est pas prise en considération si elle n'est pas intervenue plus tôt que six mois avant le dépôt de la demande de brevet européen et si elle résulte directement ou indirectement :
a) d'un abus évident à l'égard du demandeur ou de son prédécesseur en droit ou
b) du fait que le demandeur ou son prédécesseur en droit a exposé l'invention dans des expositions officielles ou officiellement reconnues au sens de la Convention concernant les expositions internationales, signée à Paris le 22 novembre 1928 et révisée en dernier lieu le 30 novembre 1972.
2) Dans le cas visé au paragraphe 1 b), ce dernier n'est applicable que si le demandeur déclare, lors du dépôt de la demande de brevet européen, que l'invention a été réellement exposée et produit une attestation à l'appui de sa déclaration dans le délai et dans les conditions prévus par le règlement d'exécution.

En application de l'article 89 « Effet du droit de priorité » de la Convention, par l'effet du droit de priorité, la date de priorité est considérée comme celle du dépôt de la demande de brevet européen pour l'application de l'article 54§2 et 3 et de l'article 60§2.

Dans ce cadre, une invention est considérée comme comprise dans l'état de la technique lorsqu'elle a été rendue accessible par et à toute personne non tenue au secret à une date certaine antérieure au dépôt de la demande de brevet ou à la date d'effet du droit de priorité. L'accessibilité est acquise dès qu'elle est théoriquement possible, aucune prise de connaissance effective n'étant à démontrer, tant

matériellement, la mise à disposition du public n'étant soumise à aucune forme et à aucune limite spatiotemporelle, qu'intellectuellement, la divulgation devant être suffisamment complète et précise pour permettre à l'homme du métier de comprendre et de reproduire l'invention à la date de cette dernière. L'élément de l'art antérieur n'est destructeur de nouveauté que s'il renferme tous les moyens techniques essentiels de l'invention dans la même forme, le même agencement et le même fonctionnement en vue du même résultat technique : l'antériorité, qui est un fait juridique dont l'existence, la date et le contenu doivent être prouvés par tous moyens par celui qui l'invoque, doit être unique et être révélée dans un document unique dont la portée est appréciée globalement.

Sur la demande de brevet européen n°0 621570 de la société France Télécom

Moyens des parties

La SA INGENICO GROUP soutient que le document EP 570 (ou France Télécom) se rapporte à un procédé de paiement entre une carte à puce prépayée et un terminal comprenant des traitements réalisés au niveau de la carte et du terminal et mettant en œuvre un protocole de paiement en plusieurs étapes imposant une liaison ou un chaînage entre des données envoyées successivement par la carte au terminal, comprenant notamment l'utilisation des données produites par la carte dans deux étapes d'authentification successives. Elle précise que les brevets EP 570 et EP 554 sont dans le même domaine d'activité, partent de postulats identiques sur les risques de fraude dans le dialogue entre la carte et le dispositif et ont des objectifs communs de sécurisation du procédé de paiement.

Elle explique que le procédé du brevet France Télécom, comme celui du brevet EP 554, comprend deux groupes d'opérations de dialogue entre la carte et le terminal, chaque groupe d'opérations (« Groupe I » et « Groupe II ») ayant des caractéristiques identiques à celles des étapes (« Step I » et « Step III ») du brevet EP 554. Elle ajoute que, dans le Groupe I, le terminal transmet un nombre aléatoire (x) à la carte (étape 6), que la carte calcule un certificat Y à l'aide du traitement F (étape 7) et qu'elle le transmet au terminal (étape 8) ce qui correspond à l'identique, au « Step I » de la revendication 1 du brevet EP 554. Elle indique que, dans le Groupe II, le terminal transmet un nombre aléatoire (x') à la carte (étape 20), que la carte calcule un certificat Y' à l'aide du traitement F (étape 21) et qu'elle le transmet au terminal (étape 22) de la même manière qu'en « Step III » de la revendication 1 du brevet EP'554. Estimant que le brevet EP'554 ne limite ni la mise en œuvre du traitement uniquement à la carte ni le nombre et la complexité des étapes ayant lieu dans ce traitement, elle précise que, dans le brevet France Télécom, le deuxième code d'authentification (Y') est, comme dans le brevet EP'554, lié au premier code d'authentification par l'utilisation d'une valeur évolutive (le compteur c) qui résulte d'un traitement effectué au moins en partie sur

la carte puisque le calcul des codes d'authentification Y et Y' sont réalisés sur la carte. Elle explique ainsi que la mise à jour du contenu de la carte nécessite, lors du premier traitement cryptographique et du Groupe I, la mise en œuvre d'une incrémentation d'une zone compteur de la carte mémoire (c) avant de pouvoir procéder à sa mise à jour. Elle précise que cette incrémentation c' (c'= c+ 1) de la zone compteur permet d'assurer qu'un certificat différent est créé à chaque utilisation de la carte, le compteur (c) de la carte mémoire étant utilisé pour éviter que les données figurant sur la carte ne soient modifiées d'une manière inappropriée voire frauduleuse. Elle en déduit que lors du Groupe II, la carte effectue, sur la base de la valeur aléatoire (x'), un calcul délivrant une valeur d'authentification Y' produite par une fonction f prenant en entrée m' (qui est le contenu de la mémoire de la carte mis à jour comprenant (b'), (c'), et (d') qui sont les nouvelles valeurs des données de transaction, de la zone compteur et d'authentification) dans laquelle la valeur c' est une deuxième valeur de départ issue du traitement précédemment réalisé entre la carte et le terminal qui participe, comme la valeur (j) correspondant à l'identité du module de sécurité du terminal, à la sécurisation des échanges.

En réplique, la société de droit néerlandais KONINKLIJKE KPN NV expose préalablement que la revendication 1 de son brevet porte sur un procédé pour réaliser une fonction particulière, c'est-à-dire « un effet » (et non pour obtenir « un produit ») et met en œuvre des éléments structurels (une carte électronique de paiement et un terminal). Elle en déduit qu'elle couvre uniquement un procédé destiné à cette fonction et utilisant des éléments structurels et ajoute qu'une telle revendication n'est comprise dans l'état de la technique que s'il contient un procédé assurant cette fonction et utilisant des éléments structurels. Elle reconnaît que la demande de brevet européen n° 0 621 570 de la société France Télécom, déposée le 14 avril 1994, publiée le 26 octobre 1994 et connue de l'examinateur lors de l'examen de sa demande de brevet, concerne un domaine technique couvert par son brevet et cherche également à résoudre un problème similaire à celui exposé dans ce dernier, à savoir améliorer la sécurité des paiements et plus particulièrement permettre au terminal de paiement de vérifier l'authenticité des montants débités de la carte de paiement.

Elle explique que le brevet de la société France Télécom enseigne d'augmenter la sécurité des transactions selon un procédé consistant notamment à mettre à jour les informations contenues dans la partie de la mémoire de la carte mémoire en incrémentant d’une unité le contenu (e) de la zone compteur avant toute mise à jour de la partie Tr de la mémoire, en ayant un certificat (d) qui est fonction de l'identité (j) du module de sécurité du terminal de paiement ayant effectué la dernière mise à jour et en faisant authentifier la carte mémoire par le terminal avant et après toute mise à jour. Elle en déduit que le compteur (c) est utilisé uniquement pour éviter que les données figurant sur la carte ne soient modifiées d'une manière inappropriée ou frauduleuse, l'utilisation combinée du compteur (c) et du certificat

(d) (avec d = g (i, b, c, j)) permettant au terminal de vérifier la cohérence des données inscrites sur la carte et de s'assurer que son contenu n'a pas été modifié d'une manière inappropriée. Elle précise que la mise en œuvre de ce procédé exige au moins trois étapes d'échanges entre la carte mémoire et le terminal dont une deuxième étape obligatoire au cours de laquelle le terminal calcule la nouvelle valeur du certificat (d), demande à la carte d'incrémenter d'une unité le contenu (c) de la zone de compteur (c'=c+1) et de réécrire dans sa mémoire les autres valeurs d'identité du module de sécurité (j'), le nouveau solde de la carte (b') et le nouveau certificat de la carte (d'). Elle ajoute que lors de la troisième étape correspondant à l'étape ultérieure de son brevet, le terminal vérifie que la valeur (j') inscrite dans la mémoire de la carte correspond bien à l'identité du module de sécurité et que c'est ce contrôle qui garantit la sécurisation des échanges. Elle en déduit, les étapes autres que l'étape initiale et l'étape ultérieure étant facultative dans son brevet qui enseigne une sécurisation en deux étapes, que le brevet France Télécom, qui ajoute une deuxième étape impliquant un calcul cryptographique complexe et qui est nécessaire à la sécurisation des échanges puisque c'est lors de celle-ci que l'identité du module de sécurité (j) du terminal est inscrite dans la carte mémoire, ne divulgue pas son procédé.

Appréciation du tribunal

La société de droit néerlandais KONINKLIJKE KPN NV est titulaire des droits de propriété intellectuelle sur le brevet européen n° 0 873 554 visant la France intitulé « méthode pour débiter un moyen de paiement électronique » dont la demande a été déposée le 14 novembre 1996 sous priorité d'une demande de brevet néerlandais n° 1 001 659 du 15 novembre 1995 et publiée le 28 octobre 1998 et qui a été délivré le 20 septembre 2000. Ayant été déposée le 14 avril 1994 et publiée le 26 octobre 1994, la demande de brevet européen n° 0 621 570 de la société France Télécom est comprise dans l'état technique.

Par ailleurs, la société de droit néerlandais KONINKLIJKE KPN NV reconnaît qu'elle couvre le même domaine technique et répond au même problème technique que son brevet, ce que confirme la lecture de la description (page 2. lignes 3 à 8 : « procédé de mise à jour d'une carte mémoire [... trouvant] une application dans ce qu'on appelle la monnaie électronique et plus particulièrement dans les systèmes à prépaiement [... impliquant] des cartes préchargées [...] et des terminaux aptes à fournir certaines prestations, à débiter les cartes en conséquence » et, pour le problème à résoudre, page 2. lignes 15 à 35 : « problèmes de sécurité », « risques de fraude » consistant en une altération ou une réutilisation des données échangées ou du contenu de la carte et en une interposition d'un autre module de sécurité).

Il est désormais acquis que :
la revendication 1 du brevet européen n° 0 873 554 couvre un procédé de sécurisation d'une transaction lors d'un dialogue entre un moyen

de paiement et un terminal de paiement par lequel la fonction de la carte génère sur la base d'une valeur aléatoire transmise par le terminal, outre un premier code d'authentification, une valeur qui sera réutilisée pour produire le second code d'authentification dans une étape ultérieure, seules ces deux étapes sont obligatoires en ce qu'elles participent à la sécurisation des échanges,
la fonction de la carte, qui n'est pas définie et peut impliquer un processus cryptographique, n'est pas revendiquée,
le procédé s'applique à une carte comprenant un solde d'unités de valeur à débiter ou à créditer,
les données de transaction transférées au terminal se limitent, codes d'authentification exceptés, aux soldes de la carte.

Si, dans le brevet européen n° 0 873 554, le terminal produit également les codes d'authentifications (page 12, lignes 8 à 14), cette opération n'est destinée qu'à la vérification des codes générés et transmis par la carte (« En comparant le code reçu avec sa contrepartie produite dans le terminal, il est possible pour le terminal de déterminer l'authenticité des données reçues et de certifier que seulement une unique carte est impliquée dans la transaction »). En revanche, tant la description que la lettre de la revendication déjà analysées révèlent que le procédé de sécurisation revendiqué repose sur les codes d'authentification générés par la carte et l'utilisation par cette dernière de la valeur finale de l'étape initiale dans la production du second code lors de l'étape ultérieure, cette valeur finale n'étant pas produite par le terminal. Le traitement F prédéterminé de la revendication 1 du brevet européen n° 0 873 554 est celui de la carte et non du terminal, la SA INGENICO GROUP ayant, au moins pour les besoins de la démonstration de la mise en œuvre d'un processus de cryptographie symétrique, admis ce raisonnement puisqu'elle explique (page 33 de ses écritures) que « la seule et unique clé qui est décrite dans le brevet et sur laquelle les revendications reposent est la clé K de la carte » qui est associée à la fonction F (description page 10, lignes 23 à 25). Le lien de dépendance qui constitue la caractéristique essentielle de la revendication est réalisée par les codes et valeurs générés par la carte, peu important que le terminal procède, à son tour et dans le seul but de vérifier les codes d'authentification transmis par la carte, aux mêmes calculs en usant de la même clé de chiffrement.

Il est par ailleurs constant que le dialogue entre le terminal et la carte ainsi que la production par celle-ci d'un code d'authentification intégrant une valeur aléatoire transmise par celui-là aux étapes initiale et ultérieure relèvent de l'état de la technique.

La demande de brevet européen n° 0 621 570 de la société France Télécom porte sur « un procédé de mise à jour d'une carte mémoire ». Après un rappel des risques connus de fraude et du coût excessif de l'insertion de microprocesseurs dans chaque carte ou de l'insuffisance de la partition des zones mémoires de la carte qui sont aisément effaçables et réinscriptibles, la description précise que l'invention

«reprend certaines opérations divulguées [...] (incrémentation d'un compteur, formation d'un certificat) » en y ajoutant « des opérations qui évitent tout risque de création de fausse monnaie » en ce que le « calcul du certificat tient compte de l'identité du module de sécurité » du terminal, le compteur est incrémenté et l'authentification de la carte par le terminal a lieu avant et après la transaction.

La demande de brevet se compose à cette fin de 4 revendications de procédé, les revendications 2 à 4 étant dépendantes de la revendication 1, et ne comporte aucune figure.

Sa revendication 1 est ainsi rédigée :
« Procédé de mise à jour d'une information (tr) contenue dans une partie (Tr) d'une mémoire (M) contenue dans une carte à mémoire (CM), à l'aide d'un terminal (T) équipé d'un module de sécurité (MS), la mémoire (M) contenant une zone compteur (C), le contenu de la partie (Tr) de la mémoire (M) à mettre **à** jour comprenant un certificat (d) contenu dans une zone (D) de la partie (Tr), ce certificat étant une fonction déterminée (g) de l'identité (i) de la carte, d'un solde (b) contenu dans une autre zone (B), du contenu (c) de la zone compteur (C), ce procédé consistant à :
incrémenter d'une unité le contenu (c) de la zone compteur (C) avant toute mise à jour de la partie (Tr),
effacer l'ancien contenu (tr) de la partie (Tr) de la mémoire (M) et y inscrire à la place un nouveau contenu (tr') mis à jour, ce procédé étant caractérisé par le fait que :
le certificat (d) est en outre une fonction de l'identité (j) du module de sécurité (MS) ayant effectué la dernière mise à jour,
pour effacer le certificat contenu dans la zone (D) et réécrire le certificat mis à jour, on incrémenté la zone compteur (C),
le terminal (T) authentifie la carte (CM) et son contenu (m) avant et après la mise à jour. »

La description comprend un mode de réalisation éclairant cette revendication décrit en ces termes :
« 1. T demande à MS de choisir un aléa ;
2. MS choisit et mémorise un aléa, soit x ;
3. MS transmet x à T ;
4. T demande à CM de lire le contenu m de la mémoire M ;
5. CM lit M et transmet m à T ;
6. T demande à CM de s'authentifier à l'aide de l'aléa x ;
7. CM calcule Y= f (m,x) ; 8 CM transmet Y a T ;
9. T transmet Y et m à MS ;
10. MS calcule f (x,m) et vérifie que Y est bien égal à f (x,m) ;
11. T demande à MS de vérifier le certificat d ;
12. MS calcule D= g (i,b,cj) ;
13. T communique à MS le débit à effectuer n ;
14. MS calcule la nouvelle valeur du solde b' =b - n, incrémenté c par c' =c + 1 et calcule d'= g(i,b',c'j') ;
15. MS transmet à T les mises à jour d', j', b' ;

16. T demande à CM d'écrire un 1 dans la zone C, d'effacer le contenu tr de la zone de travail Tr, d'y écrire le nouveau contenu tr' formé par j, b', d';
17. T demande à MS de choisir un nouvel aléa ;
18. MS choisit et mémorise un aléa x' ;
19. MS adresse x' à T;
20. T demande à CM de s'authentifier avec son nouveau contenu m' ;
21. CM calcule Y'=f (x\m');
22. CM transmet à T la valeur de Y' ;
23. T demande à MS de vérifier l'authenticité de Y' ;
24. MS vérifie que m' correspond bien à i, c', j', b', d'et vérifie que Y'= f (x',m') ;
25. si la vérification est positive, MS augmente son solde de n »
où les lettres minuscules désignent le contenu des zones mémoires identifiées par des majuscules, T est le terminal, CM la carte mémoire, m le contenu de ses données, b le solde, c le contenu de la zone compteur C, d le certificat qui est fonction de l'identité de la carte i, de b, de c et de l'identité du dernier module de sécurité ayant effectué la dernière transaction j.

Les étapes 1 à 8 puis 17 à 25 correspondent respectivement aux étapes initiale et ultérieure du brevet européen n° 0 873 554 et consistent en un dialogue connu entre le terminal doté d'un module de sécurité et la carte. En revanche, si les étapes 9 à 13 correspondent aux opérations de vérification du terminal décrites dans la description du brevet européen n° 0 873 554 (page 12, lignes 8 à 14), les étapes 14 à 16 n'ont pas d'équivalents. Cette phase intermédiaire consiste dans 1 ' incrémentation et dans le calcul du nouveau certificat opérés par le module de sécurité du terminal et dans l'instruction donnée par le terminal à la carte d'effacer sa mémoire pour y inscrire les nouvelles données relatives à l'identité du module de sécurité, au nouveau solde et au nouveau certificat. C'est précisément cette phase qui constitue le « mécanisme cliquet » qui évite tout retour en arrière (description de la demande de brevet EP 0 621 570 page 3, lignes 28 à 32).

Or, si la carte calcule les valeurs Y et Y' qui sont fonction des valeurs aléatoires transmises par le terminal et des états de sa mémoire, elle n'intervient pas dans la détermination d'une valeur finale qui sera réutilisée pour générer le second code d'authentification : seul le module de sécurité calcule ces données qui remplaceront les précédentes dans la mémoire de la carte et aucune valeur distincte du code d'authentification n'est générée par la carte lors de la phase initiale. En outre, les valeurs utilisées pour la production du second code d'authentification sont celles qui constituent la mémoire m'de la carte que sont les données mises à jour sur instruction du module du certificat, qui est notamment fonction de l'identité du module de sécurité, et du solde. Elles ne sont pas des données issues de la phase initiale produites par la fonction de la carte. Ainsi, le lien de dépendance n'apparaît que lors de la mise à jour de la carte et non dès le stade de la phase initiale par la création séparée d'un code

d'authentification et d'une valeur finale qui sera réutilisée. Elle est permise par le module de sécurité et non par la carte à la différence du brevet européen n° 0 873 554 et se réalise dans la production et la vérification des codes d'authentification.

Enfin, la valeur essentielle sur laquelle repose la sécurisation des échanges est l'identité du module de sécurité, la description précisant que la mémoire de la carte peut ne pas contenir les données du certificat et du solde, « ces données [étant] authentifiâmes indirectement par le fait que Y est une fonction notamment de (j) » (page 4, lignes 57 et 58 et page 5, ligne 1). L'incrémentation du compteur n'est sous cet angle qu'un moyen de s'assurer que cette valeur n'a pas été modifiée et qu'elle sera bien réutilisée dans la production du second code d'authentification. La valeur (j) est en conséquence celle qui permet le couplage des opérations de vérification. À supposer d'ailleurs que (c') soit la première valeur finale comme le prétend la SA INGENICO GROUP, elle n'est pas produite par la carte et est quoiqu'il en soit combinée avec (j) ce qui exclut en soi que le procédé antériorise celui du brevet litigieux.

En conséquence, l'enseignement de la demande de brevet européen n°0 621 570 de la société France Télécom est différent du brevet européen n° 0 873 554 en ce que le lien de dépendance entre les opérations de vérification est assurée, non par l'usage d'une valeur finale produite par la fonction de la carte lors de la phase initiale pour générer un second code d'authentification, mais par l'utilisation d'une valeur correspondant à l'identité du module de sécurité du terminal dont l'authenticité est garantie par une incrémentation et qui est générée par le module lui-même et inscrit dans la mémoire de la carte par une mise à jour initiée par le module dans une phase intermédiaire obligatoire.

En conséquence, la revendication 1 ne se retrouve pas dans la demande de brevet européen n° 0 621 570 et est à ce titre nouveau. Dépendantes de celle-ci, les revendications 2, 3 et 6 le sont également. La demande reconventionnelle en nullité de la SA INGENICO GROUP sera rejetée.

Sur la demande de brevet européen n° 0 637 004 de la société KPN

Moyen des parties

La SA INGENICO GROUP soutient que les brevets EP'004 et EP'554 sont dans le même domaine d'activité (un procédé de paiement entre un terminal et un poste de paiement), partent de postulats identiques (les risques de fraude dans le dialogue entre la carte et le dispositif) et ont des objectifs communs (empêcher les risques de fraude en sécurisant le procédé de paiement). Elle précise que les procédés en cause présentent deux phases d'authentification identiques et que la seconde valeur de départ est basée sur la première valeur finale

puisque les données d'usage sont réutilisées. Elle indique ainsi que le compteur de carte, qui

permet de compter le nombre d'appels et/ou le nombre des impulsions de taxation et/ou le montant des frais des appels, est produit par le traitement F et représente une valeur qui évolue dans le temps mais dont la suivante est toujours basée sur la précédente et constitue ainsi un lien entre les codes d'authentification. Elle en déduit que le brevet EP'004 divulgue la caractéristique selon laquelle la deuxième valeur de départ est dépendante de la première valeur finale.

En réplique, la société de droit néerlandais KONINKLIJKE KPN NV reconnaît que cette demande de brevet est incluse dans Fart antérieur en soulignant qu'il était visé à ce titre dans la description du brevet européen n° 0 873 554. Elle ajoute qu'elle enseigne une méthode d'enregistrement des données de transaction sur une carte à puce reposant sur au moins trois étapes qui ne comporte aucun lien entre les première et troisième étapes autre que le contrôle du solde de la carte. Elle précise ainsi que l'étape e (et l'étape h) de la demande de la demande de brevet n° 0 637 004, qui correspond à l'étape ultérieure du brevet européen n° 0 873 554, consiste en un contrôle qui s'opère sans utiliser aucune donnée provenant de l'étape initiale b car la valeur du compte de carte (le solde c) utilisée à l'étape ultérieure e (et h) ne vient pas de l'étape initiale b mais des étapes c et d assimilables à la deuxième étape optionnelle du brevet européen n° 0 873 554, n'est pas produite par la fonction F qui génère le premier code d'authentification et n'est pas la même valeur c que celle utilisée par la fonction F pour produire le premier code d'authentification.

Appréciation du tribunal

À titre liminaire, le tribunal rappelle que seules les dernières écritures des parties le lient en application de l'article 753 du code de procédure civile et qu'en conséquence, les arguments de la SA INGENICO GROUP qui renvoie à ses écritures précédentes pour l'analyse d'autres antériorités ne seront pas examinés puisqu'ils sont irréfragablement réputés abandonnés.

Ayant été déposée le 11 juillet 1994, sous priorité d'une demande de brevet néerlandaise du 20 juillet 1993 et publiée le 1er février 1995, la demande de brevet européen n° 0 637 004 de la société KPN « Méthode pour l'enregistrement de données d'utilisation de dispositifs actionnés par carte » est incluse dans l'état de la technique. Il est constant qu'elle couvre le même domaine technique et répond au même problème technique et était d'ailleurs visée en ce sens dans la description du brevet européen n° 0 873 554.

La demande de brevet comporte 2 figures et se compose de 9 revendications de procédés, les revendications 2 à 9 étant dépendantes de la revendication 1 principale qui est ainsi rédigée :

« Méthode pour l'enregistrement de façon sûre de données de prix d'une transaction d'un dispositif actionné par carte, le dispositif (2) comprenant une mémoire de dispositif (30) pour stocker des données de prix, une carte (1) comprenant une mémoire de carte (10) pour stocker un solde de carte, la méthode comprenant les étapes qui consistent à :
au début d'une transaction, transférer par la carte (1) un solde de carte initial jusqu'au dispositif (2), le dispositif stockant temporairement le solde initial, pendant la transaction, envoyer au moins une instruction de débit du dispositif à la carte (1), la carte faisant régresser le solde de carte en conséquence, à la fin de la transaction, transférer par la carte (1) un solde de carte final jusqu'au dispositif (2), le dispositif déterminant la différence entre le solde final et le solde initial et stockant ladite différence dans la mémoire de dispositif (30). »

La description précise que l'invention porte sur le « stockage sûr des données de prix dans des compteurs de téléphones publics » pour l'usage desquels une carte à puce est utilisée (page 1, lignes 14 à 18). Le procédé entend ainsi lutter contre les risques de modification des compteurs ou d'augmentation indue des soldes des cartes (page 3, lignes 21 à 28) en proposant un enregistrement fiable des données d'utilisation, en particulier des données de taxe (page 6, lignes 14 à 18). La figure 1, qui représente un échange possible de données selon l'invention entre la carte et le terminal comprenant un module de sécurité, est décrite en ces termes :
« a. La carte a été insérée dans le dispositif. À ce moment-là, le dispositif sort une instruction de marche (impulsion de marche) vers le module.
b.Entre la carte et le module se déroule une procédure de vérification par le dispositif (contrôle de l'authenticité de la carte). Cette procédure implique la transmission, entre autres, de données d'utilisation jusqu'au dispositif. Le module stocke les valeurs présentes (données d'utilisation) pour cette carte.
c. Pendant une utilisation (un appel téléphonique, une transaction d'achat), une réduction du solde de la carte a lieu (taxes de débit).
d.Comme en c.
e.La procédure de vérification est répétée dans le but de contrôler si (1) la carte est encore présente ; (2) la carte présente est authentique ; (3) la carte présente est identique à la carte présente au temps b. Le module calcule la différence entre la(les) valeur(s) présente(es) et celle(s) stockées(s) en b. et fait progresser un compteur interne. Si l'un des points (1) à (3) inclus n'est pas satisfait, la transaction est interrompue.
f. Comme en c.
g.Comme en c.
h.Comme en c.
i. La transaction est achevée, le dispositif sortant alors une instruction d'arrêt (impulsion d'arrêt) vers le module. Ce dernier peut, si c'est approprié, mettre à jour les données stockées (les contenus de compteur). »

Le processus de dialogue carte/terminal appartenant à l'art antérieur et le nombre d'étapes de vérification (2 au minimum) n'étant pas déterminé, le seul point pertinent concerne l'existence d'un lien de dépendance entre les étapes b, qui correspond à l'étape initiale, et e ou toute autre étape de vérification postérieure, qui correspond à l'étape ultérieure, lien créé par la production lors de l'étape e par une fonction de la carte d'un code d'authentification déterminé grâce à une valeur générée lors de l'étape b.

À ce titre, lors de l'étape b, la carte transmet ses données d'utilisation au dispositif qui les stocke. Elle ne produit aucune valeur autre que celle nécessaire à son authentification par le terminal, les données d'utilisation étant alors préexistantes et non générées par la fonction de la carte. Lors de l'étape e, elle transfère ces données qui comprennent (page 14, lignes 7 à 22) un code d'authenticité produit par le circuit de chiffrement sur la base d'une part d'un numéro aléatoire transmis par le terminal et d'autre part de la clé de carte, du compteur de carte et du numéro d'identification de carte, ainsi que le numéro d'identification de carte et le compteur de carte. Le module de sécurité génère à partir des mêmes éléments un code d'authentification qui sera comparé à celui produit par la carte pour s'assurer de son authenticité (page 14, lignes 23 à 35). Le numéro d'identification de la carte étant un élément constant et préexistant, la seule valeur produite susceptible de créer le lien de dépendance invoqué entre les deux opérations de vérification est le compteur. Or, les données de celui-ci ne sont ni produites ni affectées par la fonction de la carte mais uniquement par les réductions de solde opérées dans les étapes intermédiaires c et d, si bien que ses valeurs successives ne sont ni chaînées ni liées entre elles (le seul fait qu'elles correspondent à des soustractions affectant successivement le solde étant sur ce plan sans intérêt) mais dépendent des seules instructions de débit données par le terminal. La valeur du compteur, qui est une valeur dépendante de l'usage de la carte, n'étant pas comparable à la première valeur finale faute d'être générée par la fonction de la carte et conservée pour être réutilisée telle le résidu cryptographique, il est indifférent que la revendication 1 du brevet européen n° 0 873 554 vise effectivement une seconde valeur de départ « basée » sur la première valeur finale et non égale à celle-ci comme dans sa revendication 2. De ce fait, aucun lien n'existe entre les deux procédures de vérification qui sont indépendantes. C'est d'ailleurs la raison pour laquelle la description précise que la sécurisation est accrue par la répétition des opérations de vérification (page 8, lignes 4 à 10 et page 13, lignes 23 à 26) tandis que le brevet européen n° 0 873 554 ne suppose qu'une étape initiale et une étape ultérieure.

En conséquence, la revendication 1 n'est pas antériorisée par la demande de brevet n° 0 637 004 et est nouvelle. Dépendantes d'elle, les revendications 2, 3 et 6 le sont à leur tour. La demande reconventionnelle en nullité de ces revendications pour défaut de nouveauté sera en conséquence rejetée.

c) Sur l'activité inventive

Moyens des parties

La SA INGENICO GROUP explique que l'état de la technique le plus proche est le document EP 004 visé dans le brevet européen n° 0 873 554 et que la différence avec les termes de la revendication 1 réside dans le fait que la seconde valeur (Q2) de départ est basée sur la première valeur finale (Y1), cette caractéristique essentielle permettant d'assurer un lien entre le premier code d'authentification en « Step I » et le deuxième code d'authentification en « Step III » selon la demanderesse. Elle en déduit que le problème technique objectif, résolu par cette caractéristique est : « comment assurer une dépendance entre les codes d'authentification lors d'une transaction afin de s'assurer que la même carte est utilisée ? » ou « comment éviter l'indépendance entre les codes d'authentification lors d'une transaction de débit d'un moyen de paiement, afin de s'assurer que la même carte est utilisée ? », ou encore plus généralement « comment augmenter la sécurité d'une transaction entre une carte et un terminal qui comprend la génération de deux codes d'authentification successifs ? ». Elle précise que la simple formulation de ce problème démontre que la solution revendiquée est évidente et réside dans la nécessité de créer un lien entre l'étape I (Step I) et l'étape III (Step III). Elle expose que l'homme du métier sait depuis les années 1980 qu'il faut un lien, ou chaînage, et comment effectuer un tel lien. Elle liste une série de documents constituant ses connaissances générales dont elle estime que chacun d'eux, qui décrit comment effectuer un lien entre des codes d'authentification, est en mesure de faire obstacle à la brevetabilité de la revendication 1. Elle procède ensuite à une description du document « XOR MACs: New Methods for Message Authentication Using Finite Pseudorandom Functions » (ci-après BELLARE#1) publié lors d'une conférence de cryptologie en octobre 1995 et portant sur la création de codes d'authentification de messages (MAC) appelés « XOR MAC ». Elle indique que BELLARE#1 divulgue clairement l'utilisation d'une valeur de départ pour produire une valeur finale, laquelle valeur finale constitue la valeur de départ lors de l'itération suivante et en déduit que l'homme du métier, confronté au problème posé, aurait à l'évidence apporté la même solution à la simple consultation de BELLARE#1 éventuellement combiné à EP 004.

Subsidiairement, elle retient comme état de la technique le plus proche, le document EP 5704 et pose le concernant, au regard de la complexité des calculs soulevée par le brevet européen n° 0 873 554 à l'exclusion du lien effectué entre les codes d'authentification, le problème technique suivant : « comment simplifier les traitements côté terminal?». Elle conclut selon le même raisonnement et la même combinaison à l'absence d'activité inventive des revendications opposées.

En réplique, la société de droit néerlandais KONINKLIJKE KPN NV expose que le problème technique formulé par la SA INGENICO GROUP est erroné, car il procède d'un raisonnement a posteriori consistant à considérer que la solution apportée par le brevet est le problème technique posé par l'art antérieur qui était en réalité d'augmenter la sécurité des transactions réalisées à partir des moyens de paiement électroniques, le besoin d'établir un lien entre l'étape initiale et l'étape ultérieure (et a fortiori de créer ce lien en utilisant lors de l'étape ultérieure une valeur provenant de l'étape initiale) étant la solution proposée par le brevet. Elle ajoute qu'en procédant de la sorte, la SA INGENICO GROUP se dispense de démontrer que l'homme du métier aurait pensé que, pour résoudre le problème technique objectif, une solution évidente consistait à lier les codes d'authentification issus des deux étapes.

Elle explique en outre que les connaissances générales de l'homme du métier concernant les procédés cryptographiques dits de «chaînage » opposés par la SA INGENICO GROUP ne l'auraient pas incité à créer un lien entre les étapes initiale et ultérieure d'un procédé de paiement par moyen de paiement électronique, ces procédés cryptographiques ou de chiffrement, en particulier les procédés de cryptographie par blocs, concernant la façon dont un message, pour être envoyé, est découpé en blocs et dont les blocs sont liés entre eux et le chaînage des blocs composant un code d'authentification étant très différente du chaînage d'un code d'authentification à un autre. Elle précise enfin que son brevet enseigne un procédé sécurisé de paiement par carte à puce qui est indépendant des fonctions F de chiffrement utilisées pour générer les codes d'authentification MAC 1 et MAC 2.

Appréciation du tribunal

En application de l'article 56 « Activité inventive » de la Convention, une invention est considérée comme impliquant une activité inventive si, pour un homme du métier, elle ne découle pas d'une manière évidente de l'état de la technique. Si l'état de la technique comprend également des documents visés à l'article 54§3, ils ne sont pas pris en considération pour l'appréciation de l'activité inventive.

Dans ce cadre, l'état de la technique antérieur est déterminé dans les mêmes termes que celui à l'aune duquel est appréciée la nouveauté de l'invention sous réserve de l'exclusion des demandes de brevet non publiées et de la possibilité de définir cet art antérieur par la combinaison d'antériorités différentes raisonnablement envisageable pour l'homme du métier. En effet, l'élément ou les éléments de l'art antérieur ne sont destructeurs d'activité inventive que si, pris isolément ou associés entre eux selon une combinaison raisonnablement accessible à l'homme du métier, ils permettaient à l'évidence à ce dernier d'apporter au problème résolu par l'invention la même solution que celle-ci.

Publiées avant le dépôt de la demande, les deux demandes de brevet déjà examinées appartiennent à l'état de la technique.

Il est par ailleurs constant que l'état de la technique le plus proche est la demande de brevet européen n° 0 637 004 de la société KPN.

Il a déjà été dit dans le cadre de l'analyse de la portée du brevet que la nature des inconvénients prêtés à l'art antérieur et la formulation de la solution qu'entend apporter la société de droit néerlandais KONINKLIJKE KPN NV (page 4, lignes 1 à 4) révèlent que le problème technique auquel l'invention répond est celui de la sécurisation des transactions, le lien de dépendance entre les étapes d'interrogation et de production des codes d'authentification étant la réponse qui lui est donnée. En effet, lorsque la description évoque (page 3, lignes 9 à 17) l'inconvénient posé par l'indépendance des codes d'authentification, elle annonce en réalité, par une analyse orientée, la solution qu'elle entend apporter, le problème constaté étant celui de l'utilisation de plusieurs terminaux avec un moyen de paiement créant l'illusion d'une transaction complète mais non accompagnée d'un débit conséquent. L'homme du métier confronté aux risques de fraude se heurte uniquement à un problème de sécurisation des échanges, celui-ci étant nécessairement unique, peu important que seule la complexité des calculs soit invoquée à l'évocation de la demande de brevet européen n°0 621 570.

Or, s'il n'est pas contesté par la société de droit néerlandais KONINKLIJKE KPN NV que l'homme du métier sait effectuer des chaînages qui permettent d'assurer une plus grande fiabilité des procédés cryptographiques, la SA INGENICO GROUP, qui ne traite que de la première formulation de son problème technique, n'explique pas en quoi ce dernier, confronté au problème de la sécurisation des échanges entre une carte et un terminal aurait eu d'abord l'idée de recourir à un chaînage et ensuite celle de réaliser celui-ci par la production par la fonction de la carte d'une valeur lors d'une étape initiale réutilisée dans une étape ultérieure. Tous les documents cités décrivent la réalisation d'un chaînage mais n'induisent en rien le recours à ce procédé sous la forme revendiquée pour résoudre le problème posé.

Aussi, et sans qu'il soit nécessaire d'analyser le détail des antériorités invoquées, les combinaisons opérées par la SA INGENICO GROUP sont, comme l'utilisation du document BELLARE#1 seule, sans pertinence et n'apportent rien, sur le plan de l'activité inventive aux deux demandes de brevet.

Or, alors que la demande de brevet européen n° 0 621 570 de la société France Télécom enseigne une dépendance entre les opérations de vérification assurée par l'utilisation d'une valeur correspondant à l'identité du module de sécurité du terminal dont l'authenticité est garantie par une incrémentation et qui est générée

par le module lui-même et inscrit dans la mémoire de la carte par une mise à jour initiée par le module dans une étape intermédiaire obligatoire, et que la demande de brevet européen n° 0 637 004 de la société KPN divulgue une sécurisation des transactions par la répétition d'opérations de vérification indépendantes, rien ne démontre qu'il fût évident pour l'homme du métier connaisseur des procédés de chaînage de lier les codes d'authentification transmis par la carte entre eux par l'utilisation, pour générer un second code d'authentification, d'une valeur finale produite par la fonction de la carte lors de la phase initiale.

En conséquence, la revendication 1 présente une activité inventive et n'est pas nulle. Dépendantes d'elle, les revendications 2, 3 et 6 sont également inventives. La demande reconventionnelle en nullité de ces revendications présentée par la SA INGENICO GROUP sera dès lors rejetée.

2°) Sur la contrefaçon

Moyens des parties

La contrefaçon par fourniture de moyens imputée à la SA INGENICO GROUP par la société de droit néerlandais KONINKLIJKE KPN NV réside dans le fait que celle-là fournit en France, pour un usage en France, des moyens se rapportant à un élément essentiel de l'invention aptes et destinés à la mise en œuvre du procédé CDA objet de la norme

EMV. La société de droit néerlandais KONINKLIJKE KPN NV précise ainsi que :
les terminaux de paiement sont des éléments se rapportant à un élément essentiel des revendications du brevet européen n° 0 873 554 puisque la revendication 1 indique expressément que le procédé qui en est l'objet utilise un poste de paiement c'est-à-dire un terminal de paiement et que ce terminal de paiement réalise des opérations essentielles au procédé couvert par la revendication 1. peu important qu'il ne soit pas à l'origine des caractéristiques de la revendication servant de support à la nouveauté et à l'activité inventive de celle-ci et que la revendication ne porte pas spécifiquement sur les moyens fournis, la norme EMV, norme commune destinée à servir de standard international de sécurité pour les cartes à puce et les terminaux de paiement créée en 1994 à l'initiative des sociétés Europay, Mastercard et Visa et gérée par la société de droit américain EMVCo qui établit les cahiers des charges de la norme et qui délivre des certificats d'approbation des produits conformes à cette norme, met en œuvre depuis sa version V.4.1 de 2007 l'enseignement du brevet européen n° 0 873 554.

Sur ce dernier point, elle explique que le livre 2 de la norme EMV intitulé « Security and key management » présente dans le détail les

trois procédures (SDA, DDA et CDA) qui peuvent être utilisées pour vérifier l'authenticité de la carte à puce et l'intégrité des transactions, le procédé CDA étant le plus sécurisé puisque l'authentification est faite par cryptage des données avec une signature électronique et est accompagnée de l'émission d'un « application cryptogram (AC) » renvoyé par la carte au terminal en réponse à une commande « Generate AC » de ce dernier. Elle précise que ce procédé a été conçu pour être réalisé en deux étapes d'échanges (mode 1) entre la carte et le terminal qu'elle décrit ainsi :
une étape initiale débutée par l'émission par le terminal d'une première commande lst Generate AC, poursuivie par la réponse de la carte à puce par l'envoi d'un code d'authentification crypté contenant la réponse et achevée par le décryptage par le terminal du message reçu pour identifier la réponse et vérifier son intégrité, c'est-à-dire qu'il a bien été émis sur la base des données que le terminal a lui-même adressées à la carte,
une seconde étape 2nd Generate AC reprenant des échanges identiques entre la carte et le terminal avec deux différences notables :
la première tient à ce que, en réponse à la deuxième commande du terminal, la carte génère une réponse qui n'est plus une demande de connexion en ligne mais un certificat de transaction TC pour Transaction Certificate,
la seconde réside dans le fait que, pour réaliser et calculer le Transaction Data Hash Code, la carte à puce utilise la concaténation, non plus de trois séries de données, mais de quatre séries de données (les données fournies par le terminal à la carte et énumérées dans le PDOL, les données fournies par le terminal à la carte et énumérées dans le CDOL1, c'est-à-dire les données fournies avec la première commande lst Generate AC et conservées en mémoire par la carte à l'issue de la première étape, les valeurs des données fournies par le terminal à la carte et énumérées dans le CDOL2, c'est-à-dire les données fournies par le terminal à la carte avec la deuxième commande et les marqueurs, la longueur et les valeurs de certaines des informations adressées par la carte au terminal, en réponse à la seconde commande). Elle en déduit que lors du calcul du deuxième code d'authentification, la carte (et le terminal) utilisent des données CDOL1 provenant de l'étape initiale.

Elle procède enfin à l'analyse comparative des revendications opposées et de la norme EMV en précisant notamment que, à l'issue de la première étape, la carte bancaire conserve dans sa mémoire, même après l'envoi de sa réponse au terminal, les données du CDOL1 qui lui ont été fournies par le terminal et qui correspondent à la première valeur finale (Y1) de la revendication 1 en soulignant l'indifférence du fait que cette valeur ne soit pas produite par le traitement F au sens du brevet puisque la revendication 1 ne contient aucune limitation quant à la façon dont la première valeur finale (Y1), qui peut correspondre à toute valeur utilisée par la fonction F ou au résultat des calculs de la fonction F, est considérée comme produite

par cette fonction. Elle ajoute que les données du CDOL1 sont utilisées comme seconde valeur de départ dans la production par la même fonction F d'un second code d'authentification. Elle en déduit l'existence d'une reproduction littérale de la revendication et à défaut une reproduction par équivalence puisque la première valeur finale Y1 a pour fonction nouvelle de créer un lien entre l'étape initiale et l'étape ultérieure d'authentification dans le but d'augmenter la sécurité générale de la transaction et que, dans le procédé CDA, la valeur CDOL1 est utilisée pour créer un lien entre l'étape initiale et l'étape ultérieure d'authentification pour sécuriser la transaction, reproduisant ainsi la même fonction (créer un lien) en vue d'un résultat de même nature (sécuriser la transaction).

En réplique, la SA INGENICO GROUP expose en particulier que si le terminal est apte à intégrer le procédé breveté ou « apparait » dans une revendication du brevet, sa fourniture par un tiers ne constitue un acte de contrefaçon du procédé par fourniture de moyens que s'il se rapporte à la mise en œuvre d'un élément essentiel de l'invention. Elle ajoute que le terminal visé dans la revendication 1 ne fait que transmettre à la carte les valeurs aléatoires R1 puis R2 qu'il ne produit pas et souligne que ces transferts, qui relèvent d'un procédé de « challenge-réponse » bien connu de l'état de la technique figurant d'ailleurs uniquement dans le préambule de la revendication 1, ne peuvent pas être considérées comme des éléments essentiels à l'obtention du résultat. Elle précise à ce titre que l'élément essentiel de l'invention est de mettre en œuvre la liaison, dans la seconde étape du procédé, du second code d'authentification avec le premier code d'authentification, par l'utilisation d'une valeur d'entrée Q2 basée sur une valeur Y1 produite lors de la première étape d'authentification et que ce n'est pas le poste de paiement qui produit, génère et exploite la valeur finale Y1 mais le moyen de paiement qui choisit également d'utiliser une valeur d'entrée basée sur une valeur produite lors de la première étape d'authentification.

Par ailleurs, la SA INGENICO GROUP expose que les spécifications v.4.3 EMV, applicables aux cartes bancaires qui ne contiennent aucun solde, n'ont pas la même nature, ni la même fonction, ni ne poursuivent les mêmes objectifs que le brevet puisqu'elles définissent un ensemble de conditions requises pour assurer l'interopérabilité et l'acceptation de paiements sécurisés à travers le monde et pour garantir, non qu'un solde a été correctement débité, mais que les acteurs indépendants que sont la carte, le vendeur dont le terminal de paiement est utilisé et l'émetteur de la carte disposent chacun d'un état complet et exact de la transaction. Elle ajoute que « CDA » est uniquement un procédé de signature dynamique, incluant un cryptogramme et mettant en œuvre un algorithme asymétrique, qui combine :
l'authentification dynamique de la carte par le terminal au cours d'une commande unique au cours de laquelle le terminal adresse une demande GENERATE AC d'authentification à la carte qui lui répond

en générant et en adressant au terminal une signature numérique de données (« signed dynamic application data »),
la génération d'un cryptogramme par la carte au moyen d'un algorithme asymétrique à partir des données de la transaction.

Elle ajoute que la méthode CDA n'est pas obligatoire, ne représente qu'une partie d'une transaction avec une carte bancaire EMV que les spécifications EMV décrivent pour exécuter celle-ci de façon protégée et n'est pas caractérisée par une liaison spécifique de codes d'authentification. Elle conteste point par point la reproduction des caractéristiques de la revendication 1 par le procédé CDA et précise, au titre du lien de dépendance entre les deux étapes, que le 2nd GENERATE AC n'est nécessaire que lorsque l'authentification nécessite d'interroger le serveur bancaire (transaction online) et est indépendant de la première phase et que les données CDOL1 sont des données d'entrée de la première phase transmises par le terminal et ne sont pas produites par une fonction de la carte, l'algorithme CD A lui-même ne contenant qu'une seule sortie 9F4B (« Signed Dynamic Application Data ») qui ne peut fonder un chaînage des opérations. Elle en déduit l'indépendance des deux étapes.

Appréciation du tribunal

En application de l'article 64 « Droits conférés par le brevet européen » de la Convention :
1. Sous réserve du paragraphe 2, le brevet européen confère à son titulaire, à compter de la date à laquelle la mention de sa délivrance est publiée au Bulletin européen des brevets et dans chacun des États contractants pour lesquels il a été délivré, les mêmes droits que lui conférerait un brevet national délivré dans cet État.
2. Si l'objet du brevet européen porte sur un procédé, les droits conférés par ce brevet s'étendent aux produits obtenus directement par ce procédé.
3. Toute contrefaçon du brevet européen est appréciée conformément à la législation nationale.

Et, en application de l'article L 613-4 du code de la propriété intellectuelle :
1. Est également interdite, à défaut de consentement du propriétaire du brevet, la livraison ou l'offre de livraison, sur le territoire français, à une personne autre que celles habilitées à exploiter l'invention brevetée, des moyens de mise en œuvre, sur ce territoire, de cette invention se rapportant à un élément essentiel de celle-ci, lorsque le tiers sait ou lorsque les circonstances rendent évident que ces moyens sont aptes et destinés à cette mise en œuvre.
2. Les dispositions du 1 ne sont pas applicables lorsque les moyens de mise en œuvre sont des produits qui se trouvent couramment dans le commerce, sauf si le tiers incite la personne à qui il livre à commettre des actes interdits par l'article L 613-3.

3. Ne sont pas considérées comme personnes habilitées à exploiter l'invention, au sens du 1, celles qui accomplissent les actes visés aux a, b et c de l'article L 613-5.

Cette disposition est dérogatoire au droit commun en ce qu'elle permet de sanctionner l'offre de livraison ou la livraison d'un moyen qui ne reproduit pas en lui-même les revendications du brevet et n'entre de ce fait pas en principe dans le champ de la protection du brevet défini à l'article 69 de la Convention. Cette extension de la protection conférée par le titre commande l'interprétation stricte des 5 conditions auxquelles son application est subordonnée et qui résident dans le défaut d'autorisation du titulaire, la localisation en France des actes de livraison ou d'offre de livraison, le défaut d'habilitation du destinataire de celle-ci, l'existence de moyens de mise en œuvre sur le territoire français de l'invention se rapportant à un élément essentiel de celle-ci ainsi que dans la connaissance par celui qui fournit les moyens de ce que ceux-ci sont aptes et destinés à cette mise en œuvre.

Il est désormais acquis que :
la revendication 1 du brevet européen n° 0 873 554 couvre un procédé de sécurisation d'une transaction lors d'un dialogue entre un moyen de paiement et un terminal de paiement par lequel la fonction de la carte génère sur la base d'une valeur aléatoire transmise par le terminal, outre un premier code d'authentification, une valeur qui sera réutilisée pour produire le second code d'authentification dans une étape ultérieure, seules ces deux étapes sont obligatoires en ce qu'elles participent à la sécurisation des échanges.
la fonction de la carte, qui n'est pas définie et peut impliquer un processus cryptographique, n'est pas revendiquée, le procédé s'applique à une carte comprenant un solde d'unités de valeur à débiter ou à créditer.
les données de transaction transférées au terminal se limitent, codes d'authentification exceptés, aux soldes de la carte.

Les faits imputés à la SA INGENICO GROUP consistent en la vente de terminaux de paiement conformes à des normes mettant en œuvre le procédé breveté. Or. indépendamment même du fait que l'invention porte sur la sécurisation des transactions comportant l'usage de cartes intégrant un solde et non des cartes bancaires, son élément essentiel, qui réside dans le lien de dépendance unissant le second code d'authentification au premier qui est le seul élément nouveau et inventif assurant la sécurité recherchée, est réalisé uniquement par la fonction, non définie et non revendiquée, de la carte. Aux termes du brevet européen n° 0 873 554 et en particulier de sa revendication 1, le rôle du terminal se limite à l'envoi à la carte d'une valeur aléatoire pour initier chaque étape d'authentification. Cette phase, qui relève de l'art antérieur, n'est pas nouvelle. Aussi, s'il est exact que la première valeur finale est calculée pour partie sur la base de cette valeur aléatoire, l'élément essentiel consiste non dans cet usage mais dans la conservation du résidu cryptographique issu du traitement comme première valeur finale et qui servira de base au second code,

processus auquel le terminal est totalement étranger, le seul fait qu'il soit cité dans la revendication 1, et d'ailleurs dans la partie qui aurait dû constituer son préambule, étant indifférent.

L'invention couverte par la revendication 1 est mise en œuvre par la fonction de la carte, qui fait l'objet des revendications de produit, et non par le terminal qui ne participe pas à son résultat, la valeur aléatoire n'étant pas nécessaire à la dépendance entre les deux étapes initiale et ultérieure.

En conséquence, peu important l'éventuelle reproduction littérale ou par équivalence des revendications du brevet par les normes EMV, le moyen fourni par la SA INGENICO GROUP, soit le terminal, n'est pas apte à produire le résultat de l'invention et ne porte pas sur un élément constitutif de celle dernière. A ce seul égard, les demandes de la société de droit néerlandais KONINKLIJKE KPN NV au titre de la contrefaçon doivent être rejetées, les revendications 2, 3 et 6 étant dépendantes.

En outre, dans le procédé CDA des normes EMV 4.3 (livre 2. chapitre 6.6), les données CDOL1 sont transmises par le terminal à la carte lors du 1st GENERATE AC, ce que reconnaît la demanderesse dans ses écritures (page 89), puis réutilisées lors du 2nd GENERATE AC. Or, outre le fait que la CDOL1 est une donnée d'entrée et qu'elle n'est par définition pas produite par une fonction, quelle qu'elle soit, de la carte, aucune transformation de ces données n'est décrite. La société de droit néerlandais KONINKLIJKE KPN NV le reconnaît dans ses écritures lorsqu'elle écrit (page 90) que « la seconde différence notable entre les échanges intervenant à l'occasion de la deuxième commande 2nd Generate AC tient à ce que, pour réaliser et calculer le Transaction Data Hash Code, la carte à puce utilise la concaténation, non plus de trois séries de données, mais de quatre séries de données : les données fournies par le terminal à la carte et énumérées dans le PDOL, les données fournies par le terminal à la carte et énumérées dans le CDOL1, c'est-à-dire les données fournies avec la première commande 1st Generate AC et conservées en mémoire par la carte à l'issue de la première étape, les valeurs des données fournies par le terminal à la carte et énumérées dans le CDOL2, c'est-à-dire les données fournies par le terminal à la carte avec la deuxième commande, les marqueurs, la longueur et les valeurs de certaines des informations adressées par la carte au terminal, en réponse à la seconde commande ». Elle admet ainsi qu'aucune valeur produite par la fonction de la carte n'est réutilisée pour générer le certificat de transaction, la sauvegarde pure et simple d'une donnée d'entrée n'étant en rien assimilable à la production d'une donnée nouvelle, même seulement pour partie, de sortie qui sera alors sauvegardée dans la perspective de sa réutilisation. Ainsi, le seul lien identifiable entre les deux opérations est le fait du terminal et non celui d'une fonction de la carte. Et, en l'absence de production d'une donnée lors de la première étape en plus du premier code, le procédé CDA ne

reproduit pas la même fonction. Dès lors, les normes EMV ne reproduisent ni littéralement ni par équivalence la revendication 1 du brevet et les revendications dépendantes 2, 3 et 6.

Pour cette autre raison, les demandes de la société de droit néerlandais KONINKLIJKE KPN NV doivent être intégralement rejetées.

3°) Sur les demandes accessoires

Succombant au litige, la société de droit néerlandais KONINKLIJKE KPN NV, dont la demande au titre des frais irrépétibles sera rejetée, sera condamnée à payer à la SA INGENICO GROUP la somme de 200 000 euros en application de l'article 700 du code de procédure civile, ainsi qu'à supporter les entiers dépens de l'instance qui seront recouvrés directement par la SELARL CVS prise en la personne de Maître François H en application de l'article 699 du code de procédure civile.

PAR CES MOTIFS

Le tribunal, statuant publiquement, par jugement contradictoire, rendu en premier ressort et mis à la disposition par le greffe le jour du délibéré,

Rejette la demande reconventionnelle en nullité des revendications 1, 2, 3 et 6 de la partie française du brevet européen n° 0 873 554 présentées par la SA INGENICO GROUP tant au titre du défaut de nouveauté qu'à celui du défaut d'activité inventive ;

Rejette les demandes de la société de droit néerlandais KONINKLIJKE KPN NV au titre de la contrefaçon par fourniture de moyen des revendications 1, 2, 3 et 6 de la partie française du brevet européen n° 0873 554 ;

Rejette la demande de la société de droit néerlandais KONINKLIJKE KPN NV au titre des frais irrépétibles :

Condamne la société de droit néerlandais KONINKLIJKE KPN NV à payer à la SA INGENICO GROUP la somme de DEUX CENT MILLE euros (200 000 €) en application de l'article 700 du code de procédure civile ;

Condamne la société de droit néerlandais KONINKLIJKE KPN NV à supporter les entiers dépens de l'instance qui seront recouvrés directement par la SELARL CVS prise en la personne de Maître François H en application de l'article 699 du code de procédure civile.