BUNDESPATENTGERICHT

IM NAMEN DES VOLKES

URTEIL

Verkündet am
13. Juli 2004
…

4 Ni 18/03 (EU)

(Aktenzeichen)

In der Patentnichtigkeitssache

…

betreffend das europäische Patent 0 252 850
(= DE 37 81 612)

hat der 4. Senat (Nichtigkeitssenat) des Bundespatentgerichts auf Grund der mündlichen Verhandlung vom 13. Juli 2004 unter Mitwirkung des Richters Müllner als Vorsitzenden, des Richters Dipl.-Ing. Obermayer, der Richterin Schuster sowie der Richter Dipl.-Phys. Dr. Hartung und Dipl.-Phys. Dr. Zehendner

für Recht erkannt:

1. Das europäische Patent 0 252 850 wird mit Wirkung für das Hoheitsgebiet der Bundesrepublik Deutschland für nichtig erklärt.

2. Die Beklagte trägt die Kosten des Rechtsstreits.

3. Das Urteil ist gegen Sicherheitsleistung in Höhe von 120% des zu vollstreckenden Betrages vorläufig vollstreckbar.

Tatbestand

Die Beklagte ist eingetragene Inhaberin des auch mit Wirkung für die Bundesrepublik Deutschland erteilten europäischen Patents 0 252 850 (Streitpatent), das am 9. Juli 1987 unter Inanspruchnahme der Priorität der französischen Patentanmeldung 8610206 vom 11. Juli 1986 angemeldet worden ist. Das in der Verfahrenssprache Französisch veröffentlichte Streitpatent, das beim Deutschen Patent- und Markenamt unter der Nummer 37 81 612 geführt wird, betrifft ein Verfahren zum Beglaubigen der Echtheit von Daten, ausgetauscht durch zwei Vorrichtungen, die örtlich oder entfernt mittels einer Übertragungsleitung verbunden sind. Es umfasst 4 Ansprüche, von denen Patentanspruch 1 folgenden Wortlaut hat:

Verfahren zum Beurkunden der Echtheit eines Datenwerts, der zwischen einer Sende- und einer Empfangsvorrichtung ausgetauscht wird, die über einen herkömmlichen Übertragungskanal miteinander verbunden sind, wobei jede Vorrichtung über mindestens einen Speicher und Verarbeitungsschaltungen verfügt, dadurch gekennzeichnet, daß es folgende Schritte aufweist:

Erstellen einer chiffrierten Nachricht (M) auf der Ebene der Sendevorrichtung (2) durch Abarbeiten eines ersten Programms (P2), das durch erste Verarbeitungsschaltungen (T2) ausgeführt wird und das eine Chiffrierfunktion (f2) eines nichtsingulären Algorithmus mindestens auf den Chiffrierschlüssel S2 dieses Algorithmus und auf einen ersten Parameter X in solcher Weise anwendet, daß die Nachricht M eine Funktion zumindest des Chiffrierschlüssels und des ersten Parameters ist, wobei der Chiffrierschlüssel S2 des Algorithmus im Speicher (M2) der Sendevorrichtung (2) vorabgespeichert ist und der erste Parameter X in mindestens ein erstes Feld (X1), das einer vorgegebenen Bedingung genügt, und ein zweites Feld (X2) aufgeteilt ist, das für den Wert (v) des Datenwerts (d) repräsentativ ist,

das weiterhin folgende Schritte aufweist:

Übertragen der Nachricht M zur Empfangsvorrichtung (1) und Abarbeiten eines zweiten Programms (P1), das von zweiten Verarbeitungsschaltungen (T1) ausgeführt wird, um die Dechiffrierfunktion f1 des genannten Algorithmus zumindest auf die Nachricht M und den im Speicher (M1) der Empfangsvorrichtung (1) vorabgespeicherten Dechiffrierschlüssel S1 anzuwenden, um einen zweiten Para-

meter X' zu erhalten, der demgemäß eine Funktion der Nachricht M und des Dechiffrierschlüssels ist;

Zerlegen des zweiten Parameters X' in mindestens ein erstes Feld (X'1) und ein zweites Feld (X'2) und Verifizieren, daß das erste Feld (X'1) des zweiten Parameters X' derselben vorgegebenen Bedingung genügt wie das erste Feld (X1) des ersten Parameters X, um hieraus abzuleiten, daß der Wert des Datenwerts des zweiten Feldes (X'2) des zweiten Parameters mit dem Wert des Datenwerts (d) des zweiten Feldes (X2) des ersten Parameters X übereinstimmt.

Wegen der unmittelbar und mittelbar auf Patentanspruch 1 zurückbezogenen Patentansprüche 2 bis 4 wird auf die Streitpatentschrift verwiesen.

Die Klägerin behauptet, die Lehre des Streitpatents sei nicht neu bzw beruhe nicht auf einer erfinderischen Tätigkeit. Zur Begründung beruft sie sich unter anderem auf folgende Druckschriften:

EP 0 096 599 B1 (Anlagen N6 und N6a)
Meyer/Matyas, Cryptography: A New Dimension in Computer Data Security, 1982 (Anlagen N11 und N11a)
EP 0 037 762 B1 (Anlagen N12 und N12a)

Die Klägerin beantragt,

das europäische Patent 0 252 850 mit Wirkung für das Hoheitsgebiet der Bundesrepublik Deutschland für nichtig zu erklären.

Die Beklagte beantragt,

die Klage abzuweisen.

Sie ist dem Vorbringen der Klägerin entgegengetreten und hält das Streitpatent für bestandsfähig.

Entscheidungsgründe

Die zulässige Klage, mit der der in Artikel II § 6 Abs 1 Nr 1 IntPatÜG, Artikel 138 Abs 1a iVm Artikel 54 und 56 EPÜ vorgesehene Nichtigkeitsgrund der mangelnden Patentfähigkeit geltend gemacht wird, ist begründet.

1. Die Erfindung betrifft ein Verfahren zum Beglaubigen der Echtheit von Daten, die zwischen zwei Vorrichtungen ausgetauscht werden, die örtlich oder entfernt mittels einer Übertragungsleitung miteinander verbunden sind. Sie findet insbesondere Anwendung auf Speicherkarten, die mit einer externen Vorrichtung fernverbunden sind, um durch die Karte die Echtheit eines von der externen Vorrichtung übertragenen Datenwerts zu beglaubigen oder um durch die externe Vorrichtung die Echtheit eines von der Karte übertragenen Datenwerts zu beglaubigen.

Nach der Patentbeschreibung werden bei der Anwendung von Speicherkarten meistens klassische Schreib- und Leseabläufe für Daten im Speicher der Karte ausgeführt. Die Gültigkeit der Abläufe setze die Echtheit der zwischen der Karte und der externen Vorrichtung ausgetauschten Daten voraus, das heißt, dass ein empfangener Datenwert genau mit einem ausgegebenen Datenwert übereinstimmen müsse. Diese Echtheit sei jedoch nicht garantiert, da die Karte und die externe Vorrichtung durch einen klassischen Übertragungskanal fernverbunden seien, der einem Fälscher die Möglichkeit eröffne, den Datenwert während der Übertragung zu ändern. Dieses Problem, das insbesondere bei Bankanwendungen eine Rolle spiele, könne man dadurch lösen, dass man die zu übertragenden

Daten chiffriere. Diese Lösung sei jedoch nicht zufriedenstellend, da nicht sicher sei, dass der empfangene Datenwert tatsächlich dem ausgegebenen entspreche.

Nach der Patentbeschreibung ist im Stand der Technik ein Verfahren bekannt, mit dem das genannte Problem gelöst werden soll, indem die Daten in zwei getrennten Vorrichtungen auf Grundlage desselben Algorithmus berechnet würden, wobei sie den zu beglaubigenden Kartenwert, seine Adresse und Position im Speicher und einen Geheimcode berücksichtigten, den die beiden Vorrichtungen kennen. Das von der zweiten Vorrichtung berechnete Ergebnis werde zur ersten übertragen, um dort mit demjenigen verglichen zu werden, dass von der ersteren berechnet worden sei. Die Echtheit werde von der ersten Vorrichtung dann beglaubigt, wenn die zwei Ergebnisse übereinstimmten. Demgemäß setze dieses Verfahren voraus, dass die Vorrichtung, die die Bestätigung der Echtheit ausstelle, vorab die Speicheradresse und den Wert des Datenwerts kenne, den sie beglaubigen solle.

Die Erfindung lindere diesen Nachteil und erlaube es, die Echtheit eines empfangenen Datenwerts nicht nur dahingehend zu bestätigen, dass er mit dem abgegebenen Datenwert übereinstimme, sondern dies auch für einen solchen, der von einer ermächtigten Sendevorrichtung ausgegeben worden sei. So erlaube die Erfindung, gleichzeitig einen bei seiner Übertragung veränderten Datenwert festzustellen, wie auch einen Datenwert, der von einer nicht ermächtigten Sendevorrichtung ausgegeben worden sei.

2. Patentanspruch 1 beschreibt demgemäß ein

   (1) Verfahren zum Beurkunden der Echtheit eines Datenwerts, der zwischen einer Sende- und einer Empfangsvorrichtung ausgetauscht wird;

   (2) Sende- und Empfangsvorrichtung sind über einen herkömmlichen Übertragungskanal miteinander verbunden;

(3) Sende- und Empfangsvorrichtung verfügen über mindestens einen Speicher sowie über Verarbeitungsschaltungen;

(4) auf der Ebene der Sendevorrichtung wird durch Abarbeiten eines ersten Programms P2 eine chiffrierte Nachricht M erstellt;

(4.1) das erste Programm P2 wird durch erste Verarbeitungsschaltungen T2 ausgeführt;

(4.2) das erste Programm P2 wendet eine Chiffrierfunktion f2 eines nicht singulären Algorithmus mindestens auf den Chiffrierschlüssel S2 dieses Algorithmus und auf einen ersten Parameter X an;

(4.3) die Anwendung der Chiffrierfunktion f2 erfolgt so, dass die Nachricht M eine Funktion zumindest des Chiffrierschlüssels S2 und des ersten Parameters X ist;

(5) der Chiffrierschlüssel S2 des Algorithmus ist vorab im Speicher M2 der Sendevorrichtung gespeichert;

(6) der erste Parameter X ist in mindestens ein erstes Feld X1 und ein zweites Feld X2 aufgeteilt;

(6.1) das erste Feld X1 genügt einer vorgegebenen Bedingung;

(6.2) das zweite Feld X2 ist für den Wert des Datenwerts d repräsentativ;

(7) die Nachricht M wird zur Empfangsvorrichtung übertragen;

(8) es wird ein zweites Programm P1 abgearbeitet;

(9) das zweite Programm P1 wird von zweiten Verarbeitungsschaltungen T1 ausgeführt;

(9.1) durch das zweite Programm P1 wird die Dechiffrierfunktion f1 des Algorithmus zumindest auf die Nachricht M und den im Speicher der Empfangsvorrichtung vorab gespeicherten Dechiffrierschlüssel S1 angewendet;

(9.2) wodurch ein zweiter Parameter X' erhalten wird;

(9.3) dieser zweite Parameter X' ist eine Funktion der Nachricht M und des Dechiffrierschlüssels S1;

(10) der zweite Parameter X' wird in mindestens ein erstes Feld X'1 und ein zweites Feld X'2 zerlegt;

(10.1) es wird verifiziert, dass das erste Feld X'1 des zweiten Parameters X' derselben vorgegebenen Bedingung genügt wie das erste Feld X1 des ersten Parameters X;

(10.2) daraus wird abgeleitet, dass der Wert des Datenwerts des zweiten Feldes X'2 des zweiten Parameters X' mit dem Wert des Datenwerts d des zweiten Feldes X2 des ersten Parameters X übereinstimmt.

3. Patentanspruch 1 ist nicht rechtsbeständig. Ihm steht der von der Klägerin geltend gemachte Nichtigkeitsgrund der mangelnden Patentfähigkeit entgegen. Die Klägerin hat den Senat davon überzeugt, dass der Gegenstand des Anspruchs 1 nicht auf einer erfinderischen Tätigkeit beruht. In naheliegender Weise ergab sich die Erfindung für den Fachmann am Prioritätstag aus der Entgegenhaltung N12.

Als Fachmann gilt hier ein Elektroingenieur mit Fachhochschulabschluss, der mit dem Aufbau und der Funktionsweise von Chipkarten vertraut und beruflich namentlich damit befasst ist, wie man bei einem Dialog zwischen Chipkarte und externem Gerät den Datenaustausch möglichst fälschungssicher gestalten kann.

a) Ein Verfahren, Daten durch Beurkunden der Echtheit eines Datenwertes weitgehend unverfälscht zwischen einer Sendeeinrichtung 1 und einer Empfangseinrichtung 3 auszutauschen, kennt er aus N12 (Fig 1) – Merkmal 1.

Die beiden Einrichtungen 1 und 3 sind über einen herkömmlichen Übertragungskanal 2 verbunden und verfügen über Verarbeitungsschaltungen 7, 11 sowie – bei angekoppelten tragbaren Gegenständen 4, 5, namentlich Chipkarten – über mindestens einen Speicher (4ter, 5ter) – Merkmal 3.

Auf der Ebene der Sendevorrichtung wird in 7 durch Abarbeiten eines ersten Programms eine chiffrierte Nachricht erstellt - Merkmale 4 und 4.1. Es wendet eine Chiffrierfunktion eines nicht singulären Algorithmus auf den Chiffrierschlüssel R1 dieses Algorithmus und auf einen ersten Parameter an, der von einem Register 6 bis durch Verknüpfung der zu übertragenden Nachricht M mit ihrer Unterschrift SG zur Verfügung gestellt wird (N12, Sp 5 Z 26-33, Sp 5 Z 58-60; N12a, S 8 Abs 3 Satz 1, S 9 Abs 4 Satz 1) - Merkmal 4.2: Die Anwendung der Chiffrierfunktion g erfolgt so, dass die Nachricht eine Funktion zumindest des Chiffrierschlüssels R1 und des ersten Parameters ist, wobei der erste Parameter in ein erstes Feld SG und in ein zweites Feld M aufgeteilt ist - Merkmale 4.3 und 6.

Das erste Feld genügt einer vorbestimmten Bedingung, wie sie durch Verschlüsselung gemäß der Vorschrift SG = P2 (J, In, M) festgelegt und von dem tragbaren Gegenstand 4 errechnet wird (Fig 1, N 12, Sp 8 Z 10-33; N12a, S 13 Abs 3). Das zweite Feld ist für den Wert des Datenwertes M repräsentativ (N12, Sp 5 Z 45-57; N12a S 9 Abs 4) - Merkmale 6.1 und 6.2.

Bei dem bekannten Verfahren wird zwar der Chiffrierschlüssel R1 im tragbaren Gegenstand 4 an Hand der Gleichung $R_x=P_1$ (E, S, In) berechnet, wobei S und In im Speicher 4ter vorab gespeicherte geheime Parameter und E eine zufällige Zahl darstellen (N12a, S 13 Abs 3, N12 Sp 8 Z 10-13 und Anspruch 5). Es liegt aber im Bereich fachmännischen Handelns, wenn man im einfachsten Fall, mit weniger Aufwand und durch Inkaufnahme gewisser Einschränkungen der Fälschungssicherheit den Chiffrierschlüssel nicht zufallsabhängig festlegt, sondern bereits vorab im Speicher 4ter bereitstellt - Merkmal 5. Entsprechendes gilt auch im Hinblick auf die Empfangsseite (Teil aus Merkmal 9.1).

Nach Übertragung der Nachricht g (M, SG, R) zur Empfangsvorrichtung 3 findet dort ihre Entschlüsselung statt, wodurch am Ausgang der Entschlüsselungsvorrichtung 11 ein zweiter Parameter als eine Funktion der Nachricht und eines vorab gespeicherten Dechiffrierschlüssels erhalten und – im Register 14 – in ein erstes Feld SG und zweites Feld M zerlegt wird (N12 Sp 5 Z 45-57; N12a, S 9 Abs 4) - Merkmale 7 bis 10.

b) Wenn auch nach N12 nicht überprüft wird, ob das erste Feld des zweiten Parameters derselben vorgegebenen Bedingung genügt wie das erste Feld des ersten Parameters, so ist dies gleichwohl nahegelegt.

Zum einen findet sich auf dem Weg zur Erfindung als Wegmarke in N12 der Hinweis, die Unterschrift zu verifizieren (N12 Sp 3 Ziffer 2; N12a S 5 Ziffer 2). Zum andern hat der Fachmann das Ziel im Auge, beim Dialog die Fälschungssicherheit zu optimieren. Er weiß, dass er dies durch Beurkunden der Echtheit eines Datenwertes M und Mitübertragen einer davon abhängigen digitalen Unterschrift SG weitgehend erreichen kann (N12). Sein allgemeines Wissen sagt ihm aber auch, dass sich die Daten gegen betrügerische Manipulationen beim Übertragen noch besser schützen lassen, wenn man nicht nur überprüft, ob die empfangene Nachricht mit einer Unterschrift versehen ist, sondern die Unterschrift auch dahingehend untersucht, ob sie tatsächlich echt ist.

Hierzu muss verifiziert werden, ob das erste Feld des zweiten Parameters, nämlich SG, mit dem senderseitig erzeugten ersten Feld des ersten Parameters übereinstimmt, mithin derselben vorgegebenen Bedingung genügt (N12 Sp 3 Z 37-45; N12a S 5 vorle Abs iVm N12 Sp 3 Z 9-15; N12a S 4 vorle Abs). Bei Beglaubigung der Unterschrift kann man nach der Lebenserfahrung dann davon ausgehen, dass der Wert des Datenwertes des zweiten Feldes M des zweiten Parameters mit dem Wert des Datenwertes des zweiten Feldes M des ersten Parameters übereinstimmt – Merkmale 10.1 und 10.2.

An dem Ergebnis, dass der Gegenstand des Anspruchs 1 nicht auf einer erfinderischen Tätigkeit beruht, vermag auch das Vorbringen der Beklagten nichts zu ändern. Nach ihrem Verständnis weise bei der Erfindung der erste Parameter drei Felder X1, X2, X3 auf, von denen eines (X3) den Datenwert repräsentiere. Die vorbestimmte Bedingung bestehe darin, dass die beiden anderen Felder X1 und X2 identisch seien und dies bei der Verifizierung auch für die beiden entsprechenden Felder X1' und X2' des zweiten Parameters X1', X2', X3' zutreffe und demzufolge der Wert des gesendeten (X3) und empfangenen Datenwertes (X3') übereinstimmten. Für diese beschränkende Auslegung gibt der Wortlaut des Anspruchs 1 nichts her. Sie findet ihre Stütze lediglich in einer möglichen Ausführungsform nach der Patentbeschreibung (Übersetzung Streitpatentschrift N1 S 6 Abs 3 bis S 7 Abs 3). Dem Anspruch 1 darf aber nicht etwa deshalb eine einengende Auslegung zugrunde gelegt werden, weil mit dieser die Schutzfähigkeit eher bejaht werden könnte: Die vorgegebene Bedingung kann, wie aus dem oben Gesagten erhellt, ganz allgemein auch darin bestehen, dass das erste Feld SG durch die Verschlüsselung von J, In und M festgelegt ist und das restliche Feld des ersten Parameters (zweites Feld) den Datenwert M repräsentiert.

4. Die Patentansprüche 2 und 3 sind gleichfalls nicht rechtsbeständig. Auch das bekannte Verfahren enthält den Schritt, beim Verschlüsseln und Entschlüsseln eine Zufallszahl E zu berücksichtigen (Fig 1, GE 9).

Ob man diese Zufallszahl im externen Gerät, dem Sender 1, mittels eines Zufallsgenerators 9 erzeugt oder statt dessen bei jedem Gebrauch einer Chipkarte 4 aus Speicherbereichen ihres Speichers 4ter jeweils mit geändertem Wert zur Verfügung stellt, ist fachmännisches Handeln.

Schließlich prägt auch die im Anspruch 4 umschriebene Maßnahme dem Streitgegenstand nicht den Stempel einer patentfähigen Erfindung auf. Die vorgegebene Bedingung muss sende- und empfangsseitig bekannt sein. Dies trifft nach N6 beim Dialog zwischen Chipkarte und externem Gerät namentlich auch für die Adresse zu, unter der der Datenwert eingeschrieben werden soll (N6a S 6 letzter Abs und S 7 Abs 1).

5. Die Kostenentscheidung folgt aus § 84 Abs 1, 2 PatG iVm § 91 Abs 1 ZPO, die Entscheidung über die vorläufige Vollstreckbarkeit beruht auf § 99 Abs 1 PatG iVm § 709 ZPO.

Müllner Obermayer Schuster Dr. Hartung Dr. Zehendner

Fa