BUNDESPATENTGERICHT

20 W (pat) 51/01

_____

(Aktenzeichen)

Verkündet am
3. Februar 2003
…

B E S C H L U S S

In der Beschwerdesache

betreffend das Patent 195 02 657

…

hat der 20. Senat (Technischer Beschwerdesenat) des Bundespatentgerichts auf die mündliche Verhandlung vom 3. Februar 2003 durch den Vorsitzenden Richter Dr. Anders, die Richter Dipl.-Ing. Obermayer, Dr. Hartung sowie die Richterin Martens

beschlossen:

Auf die Beschwerde der Einsprechenden wird der Beschluß der Patentabteilung 31 vom 26. Juni 2001 aufgehoben und das Patent widerrufen.

G r ü n d e

I.

Das Patentamt - Patentabteilung 31 - hat das Patent mit Beschluß vom 26. Juni 2001 beschränkt aufrechterhalten. Der im Einspruch neben fehlender Patentfähigkeit ebenfalls vorgebrachte Widerrufsgrund, der Gegenstand des erteilten Patentanspruchs 1 gehe über den Inhalt der Anmeldung in der ursprünglich eingereichten Fassung hinaus, § 21 Abs 1 Nr 4 PatG, treffe nicht zu, resp dem sei durch Streichung eines der in Rede stehenden Merkmale bei dem der beschränkten Aufrechterhaltung zugrunde liegenden Anspruch 1 Rechnung getragen worden. Die Zulässigkeit des Einspruchs hat die Patentabteilung als gegeben erachtet.

Die Einsprechende stellt den Antrag,

den angefochtenen Beschluß aufzuheben und das Patent zu widerrufen.

Die Patentinhaberin beantragt,

die Beschwerde zurückzuweisen und das Patent aufrechtzuerhalten und zwar nach Maßgabe des in der mündlichen Verhandlung überreichten Anspruchs 1 sowie den dem Beschluß der Patentabteilung vom 26. Juni 2001 zugrunde liegenden Unterlagen.

Der Patentanspruch 1 - einschließlich des "Disclaimers" am Ende - lautet:

"1. Verfahren zum Nachweis einer Manipulation an Daten, die von einer in einem Fahrzeug installierten ersten Einrichtung (1) zur elektronischen Erfassung und Aufzeichnung von Daten (2), die der Überwachung der Einhaltung der Sozialvorschriften für einen Fahrerarbeitsplatz dienlich sind, unter Verwendung eines intelligenten, vorzugsweise als Chipkarte ausgebildeten mobilen Datenträgers (3), auf den Daten (2) nach dem Einbringen des Datenträgers (3) in eine Kommunikationsschnittstelle der ersten Einrichtung (1) von der ersten Einrichtung (1) übertragbar sind, auf wenigstens eine weitere zweite Einrichtung (8), die über eine Kommunikationsschnittstelle zum Auslesen und Speichern der von der ersten Einrichtung in den Datenträger (3) eingeschriebenen Daten (2) verfügt, zu übertragen sind,

gekennzeichnet durch folgende Verfahrensschritte:

a. Nach dem Einbringen eines Datenträgers (3) in die Kommunikationsschnittstelle der ersten Einrichtung (1) wird die Legitimierung des Datenträgers (3) zur Teilnahme an der Datenübertragung unter Verwendung eines sowohl in der ersten Einrichtung (1) als auch im Datenträger (3) hinterlegten Passwortes (5) geprüft.

b. Bei einem positiven Prüfungsergebnis erteilt der Datenträger (3) der ersten Einrichtung (1) das Schreibrecht, woraufhin die erste Einrichtung (1) einen oder mehrere in ihr gespeicherte und an eine weitere zweite Einrichtung (8) zu übertragende Datensätze sendet.

c. Die erste Einrichtung (1) fordert dann den Datenträger (3) auf, ein Authentifikationsmerkmal (7) aus den übertragenen Daten (2) unter Zuhilfenahme eines nur im Datenträger (3) hinterlegten geheimen Schlüssels (6) zu berechnen, dieses jedem zu übertragenden Datensatz (2) hinzuzufügen und die derart um das Authentifikationsmerkmal (7) ergänzten Datensätze (2) im Datenträger (3) zu speichern, woraufhin der Datenträger (3) aus der Kommunikationsschnittstelle der ersten Einrichtung (1) entnommen werden kann.

d. Nach dem Einbringen des Datenträgers (3) in die Kommunikationsschnittstelle der zweiten Einrichtung (8) wird auch von dieser zweiten Einrichtung (8) die Legitimierung des Datenträgers (3) zur Teilnahme an der Datenübertragung geprüft.

e. Bei einem positiven Prüfungsergebnis fordert die zweite Einrichtung (8) vom Datenträger (3) einen oder mehrere der zu übertragenden, jeweils um das Authentifikationsmerkmal (7) ergänzten Datensätze (2) an, die daraufhin vom Datenträger (3) an die zweite Einrichtung (8) zur dortigen Auswertung gesendet werden, wobei das Authentifikationsmerkmal (7) eine spätere mit der zweiten Einrichtung (8) durchgeführte Manipulation an einem ursprünglich von der ersten Einrichtung (1) stammenden und mit dem Datenträger (3) übertragenen Datensatz nachweisbar macht.

Das Merkmal:

> "d. Nach dem Einbringen des Datenträgers (3) in die Kommunikationsschnittstelle der zweiten Einrichtung (8) wird auch von dieser zweiten Einrichtung (8) die Legitimierung des Datenträgers (3) zur Teilnahme an der Datenübertragung geprüft."
>
> ist in der ursprünglichen Anmeldung nicht offenbart."

Die Patentinhaberin vertritt die Auffassung, der Merkmalsinhalt des geltenden Anspruchs 1 in der beantragten Fassung sei in den ursprünglichen Anmeldungsunterlagen als zur Erfindung gehörend offenbart worden - hiervon nimmt sie das Merkmal d. durch einen entsprechenden Hinweis aus -, und der Anspruchsgegenstand sei auch gegenüber dem Stand der Technik patentfähig.

Die Einsprechende ist nach wie vor der Auffassung, daß der beanspruchte Gegenstand in Anbetracht des durch die im Verfahren befindlichen Druckschriften belegten Standes der Technik nicht auf erfinderischer Tätigkeit beruhe. Zur Zulässigkeit des geltenden Anspruchs 1 erhebt sie keine Einwände.

Die Zulässigkeit des Einspruchs war im Beschwerdeverfahren unstrittig. Sie ist auch nach Auffassung des Senats gegeben.

In der mündlichen Verhandlung wurden u. a. folgende Entgegenhaltungen erörtert:

(2) WIGAND, Winfried: Die Karte mit dem Chip; Verlag Siemens Aktiengesellschaft, Berlin und München, 1991, Seiten 70 bis 84, und

(10) EP 0 191 413 B1.

II.

Die Beschwerde führt zum Erfolg. Das Patent kann in der beantragten Fassung nicht aufrechterhalten werden.

Der Patentanspruch 1 ist mangels Patentfähigkeit seines Gegenstands nicht rechtsbeständig (§ 21 Abs 1 Nr 1 PatG).

Für die Prüfung auf Patentfähigkeit bleibt das ursprünglich nicht offenbarte und von der Patentinhaberin in einem Zusatz zum Anspruch 1 entsprechend gekennzeichnete Merkmal d. unberücksichtigt.

Die Frage, ob der Anspruch 1 auch hinsichtlich weiterer Merkmale über den Inhalt der ursprünglichen Fassung der Patentanmeldung hinausgeht, sowie auch die Frage der Neuheit des Anspruchsgegenstandes können dahinstehen. Jedenfalls beruht der Anspruchsgegenstand nicht auf erfinderischer Tätigkeit. Er ergab sich für den Fachmann, hier ein Hochschulingenieur der Fachrichtung Nachrichtentechnik mit besonderen Kenntnissen auf dem Gebiet der Datensicherheit, insbesondere im Zusammenhang mit der Nutzung von Chipkarten, in naheliegender Weise aus dem Stand der Technik nach (10) in Verbindung mit seinem durch die Druckschrift (2) belegten Fachwissen.

Aus der Druckschrift (10) ist ein Verfahren mit den Merkmalen im Oberbegriff des Anspruchs 1 als bekannt entnehmbar, vgl die in einem Fahrzeug installierte erste Einrichtung 1 (Fahrtschreiber, Fig 1 und 3, S 4 Z 24-28, S 4 Z 53 bis S 5 Z 7), den als Chipkarte ausgebildeten mobilen Datenträger 6, 7 (Fig 2 und 3, S 5 Z 8-15), der in eine Kommunikationsschnittstelle 32, 33 (S 5 Z 6-7) der ersten Einrichtung eingebracht wird, wobei Daten - die der Überwachung der Einhaltung der Sozialvorschriften für einen Fahrerarbeitsplatz dienlich sind (S 2 Z 3-16) - als Datensätze (S 4 Z 38, S 5 Z 50-52) von der ersten Einrichtung auf den mobilen Datenträger übertragbar (Anspruch 1, S 8 Z 49 bis S 9 Z 7) und weiter auf eine zweite Einrich-

tung - eine zentrale Fuhrpark-EDV zum Auslesen und Auswerten der Daten (S 4 Z 8-16) - zu übertragen sind.

Des weiteren ist dem Fachmann aus der Druckschrift (10) auch die Problematik bekannt, daß die mittels der ersten Einrichtung auf den Datenkarten aufgezeichneten Daten den Interessen der Fahrer, der Transportunternehmer und der behördlichen Kontrollorgane gerecht werden sollen und damit auch den daraus resultierenden Interessenkonflikten ausgesetzt sind und deshalb der Gefahr der Manipulation unterliegen (S 2 Z 8-16, S 3 Z 50-53). In diesem Zusammenhang entnimmt der Fachmann aus der (10) nicht nur den allgemeinen Hinweis, daß Chipkarten an sich mehr Stör- und Fälschungssicherheit aufweisen (S 4 Z 1-3), sondern er erfährt auch, daß der Mikrocontroller der Chipkarte Programmabläufe enthält, die der Datenverschlüsselung dienen, und daß dieser Mikrocontroller dahingehend genutzt werden kann, daß Funktionen des Mikroprozessors des Fahrtschreibers - der ersten Einrichtung - in die Chipkarte verlegt werden (S 5 Z 15-18).

Die für die in Rede stehenden Daten real bestehende Manipulationsgefahr ist im Verein mit den in (10) angesprochenen Möglichkeiten der Chipkarten zur Anwendung kryptologischer Methoden für den Fachmann Veranlassung, geeignete Sicherheitsmaßnahmen und -verfahren für die Daten selbst, aber auch für deren Übertragung und Verarbeitung ins Auge zu fassen. Als Fachmann, der mit kryptologischen Verfahren im Zusammenhang mit Chipkarten vertraut ist, hat er dabei nicht nur die in (10) konkret angesprochene Datenverschlüsselung im Blick, sondern auch die zB in (2), Seiten 75 bis 78, gemeinsam mit letzterer unter dem Oberbegriff "Kryptologische Grundlagen" geschilderten Authentifikations-Verfahren, bei denen die Daten unter Verwendung eines geheimen Schlüssels mit einem Authentifikationsmerkmal (MAC) ergänzt werden, das zum Schutz der Daten gegen bewußte Veränderung (Manipulation) dient (S 77, 1. bis 3. Abs). Nachdem es dem Fachmann bei dem aus (10) bekannten Verfahren vorrangig um die Verhinderung von Manipulationen, also um die Echtheit der Daten, und weniger um die Geheimhaltung (Verschlüsselung) der Daten geht und überdies Authentifikations-

verfahren weniger Aufwand erfordern ((2), S 77 le Abs bis S 78 1. Abs), ist für den Fachmann ein solches Authentifikationsverfahren im Vergleich zu einer Daten-Verschlüsselung das Mittel der Wahl, das er bei dem in (10) beschrieben Verfahren zum Einsatz bringt.

Nachdem der Mikrocontroller der Chipkarte nach (10) ausdrücklich dafür genutzt werden kann, (kryptologische) Funktionen des Mikroprozessors der ersten Einrichtung in die Datenkarte zu verlegen (S 5 Z 16-18), bietet es sich dem Fachmann an, den Datenträger - dessen Chip mit seinem Rechenpotential (S 5 Z 15-16) - zu nutzen, um ein Authentifikationsmerkmal mit einem im Datenträger hinterlegten geheimen Schlüssel zu berechnen, dieses jedem Datensatz hinzuzufügen und schließlich die so authentifizierten Daten im Datenträger – wie auch bei dem aus (10) bekannten Verfahren - zu speichern. Damit gelangt der Fachmann aber auch zum Schritt c. des beanspruchten Verfahrens. Die in dieser Merkmalsgruppe weiter geforderte – nicht näher spezifizierte - Aufforderung der ersten Einrichtung an den Datenträger, die vorstehend geschilderte Authentifizierung durchzuführen, sieht der Fachmann in naheliegender Weise jeweils nach einer Datenübertragung vor, wenn Daten zur Authentifizierung anstehen. Das Merkmal, daß nach Authentifizierung und Abspeicherung der Daten der Datenträger aus der Kommunikationsschnittstelle entnommen werden kann, kann die erfinderische Tätigkeit des mit Anspruch 1 beanspruchten Verfahrens ebenfalls nicht stützen. Auch gemäß Druckschrift (10) kann der Datenträger nach Abspeicherung der Daten aus der Kommunikationsschnittstelle entnommen werden.

Für die Anforderung der jeweils um das Authentifikationsmerkmal ergänzten Datensätze vom Datenträger durch die zweite Einrichtung gemäß dem Verfahrensschritt e. gelten die Ausführungen, betreffend die Aufforderung der ersten Einrichtung an den Datenträger zur Authentifizierung nach Verfahrensschritt c., in entsprechender Weise. Das Auslesen und Auswerten der auf der Datenkarte gespeicherten Daten durch eine zweite Einrichtung an sich ist – wie oben dargelegt - aus (10) als bekannt entnehmbar (S 4 Z 11-16). Schließlich kann auch das Merkmal

aus Verfahrensschritt e., "...wobei das Authentifikationsmerkmal (7) eine spätere mit der zweiten Einrichtung (8) durchgeführte Manipulation an einem ursprünglich von der ersten Einrichtung (1) stammenden und mit dem Datenträger (3) übertragenen Datensatz nachweisbar macht." die erfinderische Tätigkeit des mit Anspruch 1 beanspruchten Verfahrens nicht stützen, da die bekannte Authentifizierung von Daten gerade dem Nachweis einer Manipulation an den Datensätzen dient.

Der mit Sicherheitsmaßnahmen und –verfahren betraute Fachmann hat aber nicht nur die kryptologische Sicherung der Daten an sich in seinem Blickfeld, sondern ist sich zusätzlich und unabhängig davon auch weiterer Angriffsmöglichkeiten auf die Integrität der Daten, insbesondere aus deren Umfeld und durch die die Daten nutzenden Personen bewußt. Er kennt außerdem aus seinem Fachwissen heraus, wie es zB durch die Druckschrift (2) belegt ist, die Möglichkeiten, solchen Angriffen zu begegnen. Eine dem Fachmann geläufige Maßnahme, unberechtigte Zugriffe auf Daten zu verhindern, besteht darin, eine Legitimierung der am Umgang mit den zu schützenden Daten Beteiligten durch bspw geheime Schlüsselwörter oder Paßwörter vorzusehen, vgl (2), Seite 70, Kapitel 8.2.2 iVm Seite 71 Bild 8.2. Eine solche Legitimierung bietet sich insbesondere auch für einen Datenträger gegenüber dem mit ihm kommunizierenden System an, siehe (2) Seite 71 Bild 8.2 rechter Teil. Weil der Fachmann grundsätzlich bemüht ist, nicht nur die Daten selbst, sondern auch den Umgang mit den Daten möglichst umfassend zu sichern, wird er bei dem aus (10) bekannten Verfahren neben der Authentifizierung der Daten als zusätzliche Sicherungsmaßnahme eine Legitimierung des Datenträgers mittels eines Schlüssel- oder Paßworts gegenüber der oder den mit ihm Daten austauschenden Stellen vorsehen, wie dies in (2) dargestellt ist (aaO). Überdies weist auch der in (10) beschriebene Datenträger einen gesondert definierten Speicherbereich auf, in dem zB persönliche Daten des Fahrers abgespeichert werden (S 5 Z 31-32). Mehr als eine solche, dem Fachmann geläufige Legitimierung des Datenträgers zur Teilnahme an der Datenübertragung mittels eines Paßwortes ist aber auch durch die Schritte a. und b. des Verfahrens nach Anspruch 1 nicht ge-

fordert. Daß dazu der Datenträger in die Kommunikationsschnittstelle der ersten Einrichtung eingebracht wird, ist bereits bei dem aus (10) bekannten Verfahren vorgesehen (Fig 1 S 8 Z 54). Auch macht der Beginn der Datenübertragung und damit verbunden das Erteilen eines Schreibrechts – einer Berechtigung zum Übertragen und Abspeichern - der Daten nur Sinn nach einer erfolgreichen Legitimierung, also bei einem positiven Prüfungsergebnis.

Nachdem, wie vorstehend aufgezeigt, der einschlägige Stand der Technik, insbesondere nach dem Lehrbuchauszug (2), dem um die Sicherheit von Daten bemühten Fachmann die Erkenntnis vermittelt, sowohl die Daten selbst als auch den Umgang mit den Daten zu sichern und insbesondere die daran beteiligten Partner zu kontrollieren und gegenseitig zu legitimieren, beide Möglichkeiten jedoch unabhängig voneinander zur Sicherung der Daten eingesetzt werden können, sind auch keine überraschenden kombinatorischen Wirkungen ersichtlich, die das Vorliegen einer erfinderischen Tätigkeit stützen könnten.

Dr. Anders | Obermayer | Dr. Hartung | Richterin Martens ist in Urlaub und deswegen verhindert, zu unterschreiben.

Dr. Anders

Pr