BUNDESPATENTGERICHT

17 W (pat) 331/03

(Aktenzeichen)

Verkündet am
27. Oktober 2005
…

B E S C H L U S S

In der Einspruchssache

betreffend das Patent 198 41 886

…

…

hat der 17. Senat (Technischer Beschwerdesenat) des Bundespatentgerichts auf die mündliche Verhandlung vom 27. Oktober 2005 unter Mitwirkung des Vorsitzenden Richters Dipl.-Phys. Dr. Fritsch, sowie des Richters Dipl.-Ing. Prasch, der Richterin Eder und des Richters Dipl.-Ing. Baumgardt

beschlossen:

Das Patent DE 198 41 886 wird widerrufen.

G r ü n d e

I.

Auf die am 11. September 1998 beim Deutschen Patent- und Markenamt eingegangene Patentanmeldung 198 41 886.8 - 53, für die die innere Priorität der Anmeldung 198 02 316.2 vom 22. Januar 1998 in Anspruch genommen wird, wurde das Patent unter der Bezeichnung

"Verfahren und Vorrichtung zur Erzeugung von Paßwörtern"

erteilt. Veröffentlichungstag der Patenterteilung ist der 27. März 2003.

Gegen das Patent ist Einspruch erhoben worden mit der Begründung, das Verfahren gemäß Patentanspruch 1 des Streitpatents beruhe nicht auf erfinderischer Tätigkeit und der Gegenstand des unabhängigen Vorrichtungsanspruchs 9 sei nicht neu (§ 21 Abs 1 Nr 1 PatG in Verbindung mit §§ 3, 4 PatG). Im übrigen be-

träfen die Verfahrensansprüche 1 bis 8 „Software als solche“ und seien daher vom Patentschutz ausgeschlossen (§ 1 Abs 2 Nr 3, Abs 3 PatG).

Die Einsprechende bezieht sich in ihrer Einspruchsschrift auf die Druckschriften:

[1] DE 44 11 450 C1
[2] US 5 483 598 A
[3] US 5 432 851 A – diese drei aus dem Prüfungsverfahren, ferner:

[4] US 5 060 263 A
[5] EP 0 867 843 A2 (nachveröffentlicht, älterer Zeitrang)
[6] EP 0 262 025 A2

Nach Ablauf der Einspruchsfrist hat sie noch benannt:

[7] DE 195 02 657 C1
[8] DE 195 36 206 A1
[9] EP 0 152 024 B1
[10] EP 0 271 495 B1

Sie stellt den Antrag,

das Patent zu widerrufen.

Die Patentinhaberin beantragt,

das Patent aufrechtzuerhalten
gemäß **Hauptantrag** mit Patentanspruch 1, überreicht in der mündlichen Verhandlung, sowie Patentansprüchen 2 bis 13 und Beschreibung sowie 1 Blatt Zeichnung mit 1 Figur wie Patentschrift;
gemäß **Hilfsantrag 1** mit Patentanspruch 1, überreicht in der mündlichen Verhandlung, sowie Patentansprüchen 2 bis 4, 6 bis 13, sonstige Unterlagen wie Hauptantrag.

Nach ihrer Ansicht basiert der verteidigte Gegenstand gemäß Haupt- bzw. Hilfsantrag auf technischen Überlegungen und ist durch den entgegengehaltenen Stand der Technik weder bekannt noch nahegelegt, somit patentfähig.

Der Anspruch 1 und der formal nebengeordnete Anspruch 9 nach **Hauptantrag**, hier mit einer denkbaren Gliederung versehen, lauten:

(a) **1.** Verfahren zur Erzeugung von Schlüsselwerten,

(b1) wobei ausgehend von einem geheimen Startwert ($x_{0,c}$),
(b2) welcher zusammen mit einem geheimen Schlüssel (k(C))
(b3) in einem Computer (2) und bei einem Benutzer (C) gespeichert ist,
(b4) mittels einer Verschlüsselungsfunktion unter Einbeziehung eines vorbenutzten, insbesondere des zuletzt benutzten Schlüsselwertes ein nächster Schlüsselwert ($x_{n,c}$) berechnet wird,

(c) wobei der jeweils erzeugte Schlüsselwert als einmalig gültiges Passwort für die Zugangsberechtigung auf den Computer (2) gebildet wird,

(d1) wobei der geheime Startwert ($x_{0,c}$) und der geheime Schlüssel (k(C)) auf einem dem Benutzer (C) zur Verfügung gestellten,
(d2) als Prozessor-Chipkarte ausgebildeten Datenträger (6)
(d3) in einem gesicherten, von außen nicht zugänglichen Speicherbereich gespeichert werden,

(e) wobei auf dem Datenträger (6) mittels der genannten Verschlüsselungsfunktion unter Einbeziehung des vorbenutzten Passwortes das nächste Passwort ($x_{n,c}$) berechnet und

(f) auf den Computer (2) gegeben wird zur Überprüfung der Zugriffsberechtigung des Benutzers (C) auf den Computer (2)

(g) und wobei im Computer (2) das zuletzt benutzte Passwort dem geheimen Schlüssel (k(C)) des jeweiligen Benutzers (C) zugeordnet wird.

(o) **9.** Vorrichtung zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 8,

dadurch gekennzeichnet, dass

(p) der Computer (2) eine erste Einheit (4) zur Durchführung des Verschlüsselungsverfahrens und

(q) zweite Einheit (8) zur Erzeugung des geheimen Startwertes enthält und

(r) dass der als Prozessor-Chipkarte ausgebildete Datenträger (6) zur Durchführung des Verschlüsselungsverfahrens ausgebildet ist.

Wegen der Unteransprüche 2 bis 8 und 10 bis 13 wird auf die Streitpatentschrift verwiesen.

Der **Hilfsantrag** unterscheidet sich vom Hauptantrag lediglich durch die Einfügung **(e2)** in Merkmal (e) des Anspruchs 1:

(e1) wobei auf dem Datenträger (6) mittels der genannten Verschlüsselungsfunktion,
(e2) welche durch den geheimen Schlüssel parametrisiert ist,
(e3) unter Einbeziehung des vorbenutzten Passwortes das nächste Passwort ($x_{n,c}$) berechnet und

sowie entsprechend die Streichung von Unteranspruch 5.

II.

Der Einspruch ist form- und fristgerecht erhoben und mit nachprüfbaren Gründen versehen, somit zulässig. Er hat in der Sache auch Erfolg.

Das Streitpatent betrifft ein Verfahren und eine Vorrichtung zur Erzeugung von nur einmal verwendbaren Passworten als Zugangsberechtigung zu einem Rechner.

Dem Patent soll die Aufgabe zugrundeliegen, das Verfahren (und die Vorrichtung) derart auszubilden, dass eine sichere Authentifikation eines Benutzers durch den Rechner, insbesondere eines Serversystems, erfolgt und ein sicheres Log-in auf den Rechner ermöglicht wird (siehe DE 198 41 886 C2 Absatz [0006]).

Als Fachmann für eine solche Aufgabenstellung wird im Rahmen der Lösung durch Anspruch 1 nach Haupt- und Hilfsantrag ein Spezialist für Zugangssysteme zu Datenverarbeitungsanlagen mit mehrjähriger Berufserfahrung angesehen, dem die verschiedenen möglichen Zugangsschutzverfahren wie die Verwendung von Passworten oder gespeicherter Daten auf Datenträgern (vgl Druckschrift 4 Spalte 1 Zeile 18 – 49) vertraut sind.

A. Hauptantrag

1. Der neue Anspruch 1 ist zulässig, da er lediglich eine einteilige Fassung des Hauptanspruchs aus dem Streitpatent darstellt, ohne dass einzelne Merkmale oder die Menge an Merkmalen geändert wurden.

2. Die Streitpunkte, ob die Verfahrensansprüche 1 – 8 „Software als solche“ betreffen und deshalb vom Patentschutz ausgeschlossen sind, und ob der Gegenstand des Anspruchs 9 neu ist, können unerörtert bleiben, da der Gegenstand des Anspruchs 1 nach Hauptantrag nicht auf erfinderischer Tätigkeit beruht (vgl BGH GRUR 1991, 120 "Elastische Bandage").

Der nächstkommende Stand der Technik geht aus D4 (**US 5 060 263 A**) hervor. Sie betrifft (siehe Zusammenfassung) ein Verfahren zum Erzeugen von Einmal-Passworten im Sinne des Streitpatents, wozu der Benutzer ein Passworterzeugungsgerät (password issuing device) verwendet, welches nach einem kryptografischen Algorithmus aus dem vorherigen Passwort und weiteren Parametern ein neues Passwort erzeugt. Derselbe Algorithmus und dieselben Parameter werden im zu schützenden Rechnersystem verwendet, um das neue Passwort ebenfalls zu bestimmen und mit der Benutzereingabe zu vergleichen.

Dazu beschreibt D4 in Spalte 1 - Spalte 4 Zeile 3 die vorbekannten Grundlagen der dort patentierten Erfindung und nennt zu verschiedenen Verfahren die Vor- und Nachteile. Gemäß Spalte 3 Zeile 3 – 16 wird beim sog „semisynchronen“ Verfahren ein neues Passwort durch eine Funktion F (A, K, P) bestimmt, wobei A ein kryptografischer Algorithmus, K ein kryptografischer Schlüssel und P das vorherige Passwort ist. Davon ausgehend zeigt D4 im Vergleich mit Anspruch 1 des Streitpatents:

(a) ein Verfahren zur Erzeugung von Schlüsselwerten,

(b1) wobei ausgehend von einem *vorherigen Passwort*,

(b2) welches zusammen mit einem geheimen Schlüssel (K)

(b3) in einem Computer (siehe Figur 2: im geschützten System gespeicherte Zugangsdaten, nämlich Passwort und DES keys, den Benutzern USER 0 bis USER N zugeordnet) und bei einem Benutzer (siehe Figur 6: Blockdiagramm des Passworterzeugungsgerätes mit Schlüsselspeicher 112 und Passwortspeicher 114) gespeichert ist,

(b4) mittels einer Verschlüsselungsfunktion (Spalte 3 Zeile 10: cryptographic algorithm A) unter Einbeziehung des zuletzt benutzten Schlüsselwertes (previous password P) ein nächster Schlüsselwert (Spalte 3 Zeile 15: next password) berechnet wird,

(c) wobei der jeweils erzeugte Schlüsselwert als einmalig gültiges Passwort für die Zugangsberechtigung auf den Computer gebildet wird,

(d1) wobei *das vorherige Passwort* und der geheime Schlüssel (K) auf einem dem Benutzer zur Verfügung gestellten Datenträger (password issuing device, siehe Figur 6) gespeichert werden,

(e) wobei auf dem Datenträger mittels der genannten Verschlüsselungsfunktion unter Einbeziehung des vorbenutzten Passwortes das nächste Passwort berechnet (siehe Spalte 3 Zeile 3 – 16) und

(f) auf den Computer gegeben wird zur Überprüfung der Zugriffsberechtigung des Benutzers auf den Computer

(g) und wobei im Computer das zuletzt benutzte Passwort (PASSWORD N) dem geheimen Schlüssel (DES KEYS FOR N) des jeweiligen Benutzers (USER N) zugeordnet wird (siehe Figur 2).

Hinsichtlich des Schritts (b1) „ausgehend von einem *vorherigen Passwort*“ entnimmt der Fachmann der D4 entsprechend Spalte 8 Zeile 19 – 30, dass zur Neusynchronisation anstelle des „vorherigen Passworts“ ein Wert von Null oder ein anderer vorab festgelegter Wert verwendet werden soll. Dies entspricht erkennbar dem Ausgehen von einem „Startwert“ im Sinne der Angabe (b1) des Streitpatents. Dass der Startwert geheim sein soll, ist hier platt selbstverständlich.

Das Argument der Patentinhaberin, eine Besonderheit solle gemäß Merkmal (g) darin liegen, dass im Computer das zuletzt benutzte Passwort dem geheimen Schlüssel des Benutzers zugeordnet wird, kann ebenfalls nicht durchgreifen. Gemäß D4, Figur 2, ist nämlich zu jedem Benutzer das letzte Passwort (Spalte 6 Zeile 50 – 52: for each authorized user there is stored the last value of a dynamic password) und der geheime Schlüssel (DES KEYS 52) abgespeichert. Anders kann auch Merkmal (g) nicht verstanden werden; eine bloße Zuordnung von letztem Passwort und geheimem Schlüssel (ohne den Benutzer ebenfalls zuzuordnen) könnte zudem bei mehreren Benutzern nicht funktionieren und ist so ursprünglich auch nicht offenbart, vgl Offenlegungsschrift DE 198 41 886 A1 Anspruch 7.

Der Senat verkennt bei alledem nicht, dass die eigentliche Lehre von D4 wesentlich weiter geht und, wie die Patentinhaberin zutreffend ausgeführt hat, ein deutlich aufwendigeres, insbesondere mehrere Datenübertragungsschritte umfassendes Verfahren beschreibt. Dies geschieht aber, um ua gegenüber dem dort beschriebenen „semisynchronen“ Verfahren eine höhere Sicherheit und umfassendere Verwendungsmöglichkeit zu gewährleisten (siehe D4 Spalte 4 Zeile 6 – 14). Wenn der Fachmann nun in Kenntnis von D4 auf diese Vorteile verzichten und unter In-

kaufnahme der bekannten Nachteile zu dem dort ebenfalls beschriebenen einfacheren Verfahren zurückkehren will, kann dies eine erfinderische Tätigkeit keinesfalls begründen (vgl BGH GRUR 96, 857 (III 2c) „Rauchgasklappe“).

Das in D4 beschriebene einfachere „semisynchrone“ Verfahren entspricht somit, wie dargelegt, weitgehend dem Verfahren nach Anspruch 1 des Hauptantrags. Ein Unterschied besteht lediglich in den Merkmalen (d2) und (d3), dass gemäß Streitpatent der Datenträger (das Passworterzeugungsgerät)

(d2) als Prozessor-Chipkarte ausgebildet ist, und
(d3) das vorherige Passwort bzw. der geheime Startwert und der geheime Schlüssel in einem gesicherten, von außen nicht zugänglichen Speicherbereich gespeichert werden.

Diese Maßnahmen waren aber für den Fachmann naheliegend. Am Prioritätstag waren nämlich Prozessor-Chipkarten mit einem gesicherten, von außen nicht zugänglichen Speicherbereich und deren Verwendung für Zugangskontrollsysteme allgemein bekannt, was rein beispielhaft durch D10 belegt wird (siehe dort insbesondere Seite 2 Zeile 47 – 51 und Seite 9 Zeile 34 – 37). Es bedurfte keiner erfinderischer Überlegungen, um eine solche Prozessor-Chipkarte als Datenträger für das Verfahren gemäß D4 einzusetzen, weil bereits D4, Spalte 8, Zeile 55 – 57, von „Kreditkartengröße“ spricht. Dass die geheimzuhaltenden Daten in dem gesicherten, von außen nicht zugänglichen Speicherbereich besonders gut aufgehoben sind, versteht sich von selbst.

Somit gelangt der Fachmann, ausgehend von D4, ohne erfinderische Tätigkeit zum Gegenstand des Anspruchs 1 nach Hauptantrag. Dieser ist folglich nicht rechtsbeständig.

Da über einen Antrag nur einheitlich entschieden werden kann (vgl BGH GRUR 1997, 120 "Elektrisches Speicherheizgerät"), sind auch der nebengeordnete Anspruch 9 und die jeweiligen Unteransprüche 2 bis 8 sowie 10 bis 13 nicht rechtsbeständig.

B. Hilfsantrag

Der Anspruch 1 nach Hilfsantrag unterscheidet sich von der Fassung nach Hauptantrag einzig durch Merkmal (e2), nämlich dass die Verschlüsselungsfunktion „durch den geheimen Schlüssel parametrisiert ist“.

Zwar ist diese Einschränkung in Anspruch 1 zulässig, weil das zusätzliche Merkmal aus Anspruch 5 der erteilten Fassung des Streitpatents stammt.

Doch ist auch dieses der D4 ohne weiteres entnehmbar. Gemäß Spalte 3 Zeile 10 – 12 wird der geheime Schlüssel K mit dem kryptografischen Algorithmus A benutzt, was aus fachmännischer Sicht nichts anderes bedeutet, als dass der Algorithmus durch den Schlüssel „parametrisiert“ wird.

Die gegen die Rechtsbeständigkeit der verteidigten Anspruchsfassung nach Hauptantrag sprechenden Gründe gelten somit in gleicher Weise gegen die Fassung nach Hilfsantrag.

III.

Bei der gegebenen Sachlage war demzufolge das Patent zu widerrufen.

Dr. Fritsch Prasch Eder Baumgardt

Na