BUNDESPATENTGERICHT

19 W (pat) 44/09

_____

(Aktenzeichen)

Verkündet am
28. Juni 2010
…

B E S C H L U S S

In der Beschwerdesache

…

betreffend die Patentanmeldung 199 13 931.8-53

hat der 19. Senat (Technischer Beschwerdesenat) des Bundespatentgerichts am 28. Juni 2010 unter Mitwirkung des Vorsitzenden Richters Dipl.-Ing Bertl, der Richterin Kirschneck und der Richter Dr.-Ing. Scholz und Dipl.-Ing. Groß

beschlossen:

Der Beschluss der Prüfungsstelle für Klasse G 07 C des Deutschen Patent- und Markenamts vom 14. März 2006 wird aufgehoben und das nachgesuchte Patent mit der Bezeichnung "Überprüfungsverfahren und elektromechanisches Schließsystem" und den folgenden Unterlagen erteilt:

Patentansprüche 1 bis 13,
angepasste Beschreibung,
jeweils überreicht in der mündlichen Verhandlung,
ein Blatt Zeichnung vom Anmeldetag 26. März 1999.

G r ü n d e

I.

Das Deutsche Patent- und Markenamt – Prüfungsstelle für Klasse G 07 C - hat die Anmeldung mit dem Anmeldetag 26. März 1999 und der Bezeichnung "Überprüfungsverfahren" durch Beschluss vom 14. März 2006 mit der Begründung zurückgewiesen, dass der Gegenstand des Patentanspruchs 1 gegenüber dem Stand der Technik nicht auf einer erfinderischen Tätigkeit beruhe.

Gegen diesen Beschluss richtet sich die Beschwerde der Anmelder.

Die Anmelder beantragen,

den Beschluss der Prüfungsstelle für Klasse G 07 C des Deutschen Patent- und Markenamts vom 14. März 2006 aufzuheben und das nachgesuchte Patent mit der geänderten Bezeichnung "Überprüfungsverfahren und elektromechanisches Schließsystem" und den folgenden Unterlagen zu erteilen:

Patentansprüche 1 bis 13,
angepasste Beschreibung,
jeweils überreicht in der mündlichen Verhandlung,
ein Blatt Zeichnung vom Anmeldetag 26. März 1999.

Der gültige Anspruch 1 lautet:

"Verfahren zur Überprüfung von Berechtigungen zum Betätigen von elektromechanischen Schließsystemen, mit einer Schloßeinheit (10), mit welcher wenigstens eine von einem Benutzer mitführbare Schlüsseleinheit (12) zusammenwirkt, die eine Read-Write Transpondereinheit (14) ohne Kryptoprozessor zur berührungslosen Kommunikation mit der Schloßeinheit (10) aufweist, bei der

(a) zumindest eine einzigartige, unveränderbare, feste Identifikation (ID) der Schlüsseleinheit (12) sowie ein aus der Identifikation (ID) gemäß einem Verschlüsselungsverfahren (V) erzeugter Code (S), welcher in der Schlüsseleinheit (12) gespeichert ist, mittels der Transpondereinheit (14) an die Schloßeinheit (10) übertragen werden,

(b) in der Schloßeinheit (10) aus der übertragenen Identifikation (ID) gemäß dem Verschlüsselungsverfahren (V) erneut ein Code (S') erzeugt wird, und

(c) der gemäß Schritt (a) an die Schloßeinheit (10) übertragene Code (S) und der gemäß Schritt (b) in der Schloßeinheit (10) erzeugte Code (S') miteinander verglichen werden."

Wegen weiterer Einzelheiten wird auf den Akteninhalt verwiesen.

II.

Die Beschwerde ist statthaft und auch sonst zulässig. Sie ist insbesondere von den am Verfahren vor dem Patentamt beteiligten, nach § 74 Abs. 1 PatG beschwerdeberechtigten beiden Anmeldern eingelegt worden. Die Angabe der Firma U… & Z… als Anmelder im Beschwerdeschriftsatz vom 26. April 2006
sieht der Senat als offensichtlichen, ohne Weiteres korrigierbaren Fehler an. Dies ergibt sich zweifelsfrei aus den sonstigen eindeutigen Angaben in der Beschwerdeschrift unter Berücksichtigung der Akten des Patentamts. Die Beschwerde hat auch in der Sache teilweise Erfolg, soweit sie zur Erteilung des Patents mit den im Tenor genannten Unterlagen führt.

1. Das Patent betrifft ein Verfahren zum Überprüfen von Berechtigungen zum Betätigen von elektromechanischen Schließsystemen. Derartige Schließsysteme sind gewöhnlich mit einem Transponderchip im Schlüssel ausgerüstet, der mit der Schließanlage berührungslos kommuniziert. Die Anmeldungsbeschreibung nennt hierfür sogenannte Read-Only-Transponder, die eine unveränderbare oder feste Kennung aufweisen, und in die keine Daten hineingeschrieben werden können, des weiteren Read-Write-Transponder, sowie Krypto-Transponder, bei denen der Datenaustausch zwischen dem Schlüssel und dem Schloss verschlüsselt wird.

Read-Only-Transponder und Read-Write-Transponder werden als zu unsicher, Krypto-Transponder als zu aufwändig bezeichnet.

Hieraus ergibt sich die Aufgabe, ein Verfahren zum Überprüfen von Berechtigungen zum Betätigen von elektromechanischen Schließsystemen zu schaffen, das bei möglichst geringem Aufwand eine möglichst hohe Sicherheit gegenüber Manipulationen bietet und das insbesondere mit herkömmlicher und preisgünstiger Transpondertechnik realisiert werden kann (Sp. 2, Z. 64 bis Sp. 3, Z. 2 der eingereichten Beschreibung).

Zur Lösung dieser Aufgabe gibt der gültige Anspruch 1 ein Verfahren an, bei dem:

> "(a) zumindest eine einzigartige, unveränderbare, feste Identifikation (ID) der Schlüsseleinheit (12) sowie ein aus der Identifikation (ID) gemäß einem Verschlüsselungsverfahren (V) erzeugter Code (S), welcher in der Schlüsseleinheit (12) gespeichert ist, mittels der Transpondereinheit (14) an die Schloßeinheit (10) übertragen werden,
>
> (b) in der Schloßeinheit (10) aus der übertragenen Identifikation (ID) gemäß dem Verschlüsselungsverfahren (V) erneut ein Code (S') erzeugt wird, und
>
> (c) der gemäß Schritt (a) an die Schloßeinheit (10) übertragene Code (S) und der gemäß Schritt (b) in der Schloßeinheit (10) erzeugte Code (S') miteinander verglichen werden."

Es wird also eine für die jeweilige Transpondereinheit und Schlüsseleinheit einzigartige und unveränderbare, feste Identifikation, die der Beschreibung (Sp. 3 Z. 32 bis 39) zufolge auch als Unique Identification (UID) bezeichnet wird, zur Erzeugung eines verschlüsselten Codes herangezogen, der auf der Karte abgespeichert wird. Zur Überprüfung wird die Identifikation in der Schlosseinheit nochmals verschlüsselt und dann mit dem gespeicherten Code verglichen. Bei Übereinstimmung wird das Schloss freigegeben.

2. Für diesen Sachverhalt sieht der Senat einen Diplomingenieur (Univ.) der Fachrichtung Elektrotechnik mit Erfahrung in der Entwicklung von elektronischen Zugangsberechtigungssystemen als Fachmann.

3. Bevor der Anspruch 1 auf Patentfähigkeit geprüft werden kann, ist festzustellen, wie ihn der Fachmann versteht:

Die Ausrüstung der Schlosseinheit ist nicht definiert. Für den Fachmann ist aber klar, dass sie zumindest über eine Transponder-Schreib-Leseeinheit und einen Mikroprozessor zur Durchführung der Verschlüsselung nach Merkmal b) verfügen muss.

Die Schlüsseleinheit 12 verfügt nicht nur über einen Transponder, sondern auch über einen Speicherchip. Solche aus Transponder und Chip bestehenden Einheiten werden häufig als Transponderchip (Sp. 1, Z. 33 bis 43) oder verkürzt als Transponder (Sp. 1, Z. 63 bis 66) Read-Only-Transponder oder Read-Write-Transponder bezeichnet.

Der Forderung nach einer einzigartigen, unveränderbaren, festen Identifikation (ID) der Schlüsseleinheit nach Merkmal a) ist bereits mit einer eindeutigen Zuweisung, z. B. einer Seriennummer über eine Liste, Genüge getan. Über die Art der Abspeicherung dieser Identifikation sagt das nichts.

Der Fachmann wird aber davon ausgehen, dass derartige Identifikationen bzw. Seriennummern üblicherweise herstellerseitig unveränderbar eingespeichert sind. Sie muss sich demnach in einem anderen Speicherbereich befinden als dem nach Oberbegriff vorausgesetztem Schreib-Lese-Speicher. Für einen funktionierenden Kopierschutz muss ferner sichergestellt sein, dass eine illegale Kopie nur auf einem Transponderchip mit herstellerseitig unveränderbar eingespeicherter Identifikation/Seriennummer angefertigt werden kann, und dass dieser Chip der Schlosseinheit nicht eine andere als die eigene Identifikation/Seriennummer als Identifikation anbieten kann. Ohne diese Voraussetzungen ist das beanspruchte Verfahren zwar funktionsfähig und ausführbar, bietet aber nicht den beschriebenen Kopierschutz. Der Vertreter der Anmelder hat dazu angegeben, dass das durch physikalische Anpassung (z. B. Integration in einen speziellen mechanischen Schlüssel) oder ein entsprechendes Übertragungsprotokoll gewährleistet werden kann. Diese Maßnahmen sind aber nicht Bestandteil der Erfindung.

Nach Merkmal b) wird gemäß dem Verschlüsselungsverfahren (V) erneut ein Code erzeugt. Damit ist klargestellt, dass das Verschlüsselungsverfahren (V) in Merkmal a) und b) das gleiche ist, dass es sich also um ein symmetrisches Verschlüsselungsverfahren mit doppelter Verschlüsselung handelt.

4. Die geltenden Ansprüche 1 bis 13 sind ursprünglich offenbart (§ 38 Satz 1 PatG).

Der Anspruch 1 wurde zulässig auf Schließsysteme beschränkt. Ferner wurde die Transpondereinheit als Read-Write Transpondereinheit ohne Kryptoprozessor (offenbart auf S. 5, Abs. 2, 3 und S. 6, Z. 22 bis 28 der ursprünglichen Beschreibung), und die feste Identifikation als einzigartige, unveränderbare, feste Identifikation (offenbart auf S. 6, Z. 16 bis 18) präzisiert. Die übrigen Ansprüche sind - bis auf die Streichung zweier Ansprüche und die geänderte Nummerierung und Rückbeziehung einiger Ansprüche - unverändert.

5. Das Verfahren nach Anspruch 1 ist neu (§ 3 PatG).

Die EP 671 712 A1 beschreibt ein System zur Authentifizierung um eine Transaktion zu erlauben (Titel). Als Anwendungsgebiet sind Bankautomaten ("terminal point de vente", Sp. 3, Z. 28 bis 33) oder ähnliches für Geldtransaktionen genannt (Sp. 3, Z. 2 bis 14). Dazu ist auf einem EEPROM-Speicher 2 einer Transponder-Chipeinheit 1 eine Seriennummer Ns und ein Authentifizierungswert VA gespeichert (Sp. 2, Z. 28 bis 38). In einem Zentralrechner 4 ist eine Information I über die Berechtigungen der Karte 2, aus der ein Verschlüsselungprogramm F zusammen mit der Seriennummer Ns und einem Geheimschlüssel Ks den Authentifizierungswert VA erzeugt (Sp. 2, Z. 53 bis Sp. 3, Z. 24). An einem Terminal 8 wird nach einer ersten Variante des Verfahrens (ab Sp. 3, Z. 36) der Wert VA entschlüsselt und die Information I über die Berechtigungen wiederhergestellt. Es handelt sich dabei um ein sogenanntes asymmetrisches Verschlüsselungssystem mit einem geheimen Schlüssel Ks zur Verschlüsselung und einen öffentlichen Schlüssel Kp zur Entschlüsselung.

In einer zweiten, im Prüfungsverfahren herangezogenen Variante (ab Sp. 5, Z. 39) lässt sich der Wert Va nicht mehr entschlüsseln. Die Information I wird zusätzlich auf der Karte 2 abgespeichert. Eine Authentifikation wird anhand eines Verfahrens G mit einem öffentlichen Schlüssel KP ohne Entschlüsselung der Information I durchgeführt (Sp. 5, Z. 39 bis Sp. 6, Z. 30).

Mit den Worten des Anspruchs 1 ist damit (Abweichungen unterstrichen) bekannt ein:

> Verfahren zur Überprüfung von Berechtigungen mit einer Einheit 8, mit welcher wenigstens eine von einem Benutzer mitführbare Einheit 1 zusammenwirkt, die eine Read-Write (EEPROM) Transpondereinheit 2, 3 ohne Kryptoprozessor zur berührungslosen Kommunikation mit der Einheit 8 aufweist, bei der

(a) zumindest eine einzigartige, unveränderbare, feste Identifikation NS der Einheit 1 sowie ein aus der Identifikation NS gemäß einem Verschlüsselungsverfahren F erzeugter Code VA, welcher in der Einheit 1 gespeichert ist, mittels der Transpondereinheit 2, 3 ohne weitere Verschlüsselung an die Einheit 8 übertragen werden.

Der Auffassung, die Identifikation NS sei nicht als fest anzunehmen, weil sie in einem EEPROM abgespeichert sei, kann sich der Senat nicht anschließen. Eine Seriennummer muss schon ihrer Natur nach einzigartig, unveränderbar und fest sein. Über Art und Ort ihrer Abspeicherung sagt dies zunächst nichts. Die Annahme, dass die Seriennummer nicht im elektrisch löschbaren Bereich der Karte gespeichert ist, ist gleichermaßen angebracht wie die Annahme, dass sich bei der anmeldungsgemäßen Schlüsseleinheit die Identifizierung nicht in dem Read-Write-Bereich befindet. Hier entspricht sich die Offenbarung der Entgegenhaltung und die der Anmeldung.

Im Unterschied zum Anspruch 1 dient dieses Verfahren nicht zur Überprüfung der Schlüssel einer Schließanlage. Im Unterschied zum Merkmal b) des Anspruchs 1, wird in der zweiten Variante aus der übertragenen Identifikation NS (und dem Wert VA) gemäß einem anderen Verfahren G mit einem öffentlichen Schlüssel KS direkt eine Information über die Authentizität der Information gewonnen. Ob es sich dabei um ein Verschlüsselungsverfahren oder ein Entschlüsselungsverfahren (wie bei der ersten Variante) handelt, bleibt offen. Das Ergebnis ist weder eine verschlüsselte noch eine entschlüsselte Information, sondern lediglich die Aussage "authentisch" "oder nicht authentisch". Ein Vergleich dieses Ergebnisses mit dem Wert VA, entsprechend dem Vergleich mit dem Code S nach Merkmal c), ist weder möglich noch nötig.

Die erste Variante ermöglicht zwar - neben der ausführlicher beschriebenen Plausibilitätskontrolle der Berechtigungen I (Sp. 4, Z. 24 bis 46) - auch einen Vergleich der gespeicherten mit der entschlüsselten Identifikationssnummer Ns (Sp. 4, Z. 21 bis 24) zur Feststellung der Authentizität. Dort wird aber die Identifikationssnummer Ns bei der Entschlüsselung der Berechtigungen VA bzw. I erhalten, und es werden die unverschlüsselten Werte verglichen.

Die DE 196 03 320 C2 zeigt eine elektronische Schließanlage mit einem Transponderchip 73 in dem Schlüssel 11, der mit einem Schloss zusammenwirkt (Sp. 11, Z. 50 bis Sp. 12, Z. 12). Wird der Schlüssel in das Schloss gesteckt, sendet das Schloss an den Schlüssel einen Erkennungscode, der bei richtigem Code einen schlüsselspezifischen Code zurücksendet (Sp. 12, Z. 53 bis 68, Sp. 13, Z. 3 bis 14, 27 bis 32).

Damit ist mit den Worten des Anspruchs 1 bekannt ein:

> Verfahren zur Überprüfung von Berechtigungen zum Betätigen von elektromechanischen Schließsystemen, mit einer Schloßeinheit 14, mit welcher wenigstens eine von einem Benutzer mitführbare Schlüsseleinheit 73 zusammenwirkt, die eine Read-Write Transpondereinheit 74, 75, 81 ohne Kryptoprozessor zur berührungslosen Kommunikation mit der Schloßeinheit 14 aufweist.

Eine Verschlüsselung ist nicht vorgesehen, ebenso wenig eine unveränderbare Identifikation (Merkmale a bis c).

Die DE 41 38 861 A1 und DE 43 42 641 A1 beschreiben Authentifizierungsverfahren, bei denen der Transponderchip einen Kryptoprozessor mit einem Verschlüsselungsprogramm aufweist (DE 41 38 861 A1, Sp. 2, Z. 56 bis 58, Sp. 3, Z. 18 bis 23, Z. 63 bis Sp. 4 Z. 1; DE 43 42 641 A1, Sp. 3, Z. 8 bis 13). Der Senat sieht sie - wie die Prüfungsstelle – als weiter abliegend an.

6. Das Verfahren nach Anspruch 1 beruht auch auf einer erfinderischen Tätigkeit (§ 4 PatG).

Ausgehend von dem aus der EP 671 712 A1 bekannten Verfahren mag es nahe liegen, eine Schließanlage damit auszurüsten (Sp. 1, Z. 5, 6, Zugang zu einem Dienst oder Ort). Doch selbst wenn der Fachmann dieses Verfahren bei einer Schließanlage einsetzen würde, wäre nur Merkmal a) jedoch nicht die Merkmale b) und c) realisiert. Dafür gibt es auch keinerlei Anlass, denn das würde dem Grundgedanken der dort verwendeten asymmetrischen Verschlüsselung mit einem geheimen und einem öffentlichen Schlüssel widersprechen. Außerdem würden selbst bei gleichem Schlüssel die Informationen - die Berechtigungen VA bzw. I - entweder verschlüsselt und entschlüsselt werden (1. Variante), oder unverschlüsselt übertragen werden (2. Variante). Eine doppelte Verschlüsselung wäre bei einem System, das Informationen übertragen soll, sinnwidrig.

Um zum Verfahren nach Anspruch 1 zu kommen bedurfte es somit erfinderischer Überlegungen.

7. Der Anspruch 1 hat somit ebenso wie die auf ihn rückbezogenen Ansprüche 2 bis 9 Bestand. Für den zum Anspruch 1 inhaltsgleichen Vorrichtungsanspruch 10 mit den auf ihn rückbezogenen Ansprüchen 11 bis 13 gilt das sinngemäß.

Bertl Kirschneck Groß Dr. Scholz

Pü