BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS

BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE

CHAMBRES DE RECOURS DE L'OFFICE EUROPEEN DES BREVETS

Interner Verteilerschlüssel:
(A) [ ] Veröffentlichung im ABl.
(B) [ ] An Vorsitzende und Mitglieder
(C) [ ] An Vorsitzende
(D) [X] Keine Verteilung

Datenblatt zur Entscheidung vom 28. April 2009

Beschwerde-Aktenzeichen: T 0337/06 - 3.4.03

Anmeldenummer: 98919270.3

Veröffentlichungsnummer: 0990226

IPC: G07F 7/08

Verfahrenssprache: DE

Bezeichnung der Erfindung:
System zum gesicherten Lesen und Bearbeiten von Daten auf intelligenten Datenträgern

Patentinhaber:
Deutsche Telekom AG

Einsprechender:
GIESECKE & DEVRIENT GmbH

Stichwort:
-

Relevante Rechtsnormen:
-

Relevante Rechtsnormen (EPÜ 1973):
EPÜ Art. 56

Schlagwort:
"Erfinderische Tätigkeit (nein)"

Zitierte Entscheidungen:
-

Orientierungssatz:
-

Aktenzeichen: T 0337/06 - 3.4.03

E N T S C H E I D U N G
der Technischen Beschwerdekammer 3.4.03
vom 28. April 2009

Beschwerdeführer: (Einsprechender)
GIESECKE & DEVRIENT GmbH
Prinzregentenstr. 159
D-81677 München (DE)

Vertreter:
Klunker, Hans-Friedrich
Klunker Schmitt-Nilson Hirsch
Patentanwälte
Destouchesstraße 68
D-80796 München (DE)

Beschwerdegegner: (Patentinhaber)
Deutsche Telekom AG
Friedrich-Ebert-Allee 140
D-53113 Bonn (DE)

Vertreter:
Katscher Habermann Patentanwälte
Dolivostraße 15A
D-64293 Darmstadt (DE)

Angefochtene Entscheidung: **Zwischenentscheidung der Einspruchsabteilung des Europäischen Patentamts über die Aufrechterhaltung des europäischen Patents Nr. 0990226 in geändertem Umfang, zur Post gegeben am 28. Dezember 2005.**

Zusammensetzung der Kammer:

Vorsitzender: G. Eliasson
Mitglieder: R. Q. Bekkering
P. Mühlens

Sachverhalt und Anträge

I. Die Beschwerde richtet sich gegen die Zwischenentscheidung der Einspruchsabteilung, das Patent Nr. 0 990 226 in geändertem Umfang aufrechtzuerhalten. Einzige Beschwerdeführerin ist die Einsprechende.

II. Die Beschwerdeführerin beantragt, die angefochtene Entscheidung aufzuheben und das Patent zu widerrufen.

III. Die Beschwerdegegnerin (Patentinhaberin) beantragt die Beschwerde zurückzuweisen.

IV. Anspruch 1 lautet:

"1. System zum gesicherten Lesen und Ändern von Daten auf intelligenten Datenträgern (4), insbesondere IC-Karten, mit Terminals (2a, 2b), die einer übergeordneten Zentrale (1) zugeordnet und mit zur temporären Kommunikation mit den Datenträgern geeigneten Schnittstellen (E, D) ausgestattet sind, wobei auf jedem Datenträger neben der auszulesenden oder zu ändernden Information und einer Identifikationsinformation ein Schlüssel (K_{auth}) gespeichert ist, der auch den Terminals zur Authentikation des jeweiligen Datenträgers nach einem symmetrischen Schlüsselverfahren zur Verfügung steht, gekennzeichnet durch folgende Merkmale:
a) ein auf dem Datenträger zur Übergabe an das Terminal gespeichertes Zertifikat, das mit Hilfe einer zur Zertifizierung der im System zu verwendenden Datenträger dienenden globalen Signierfunktion (S_{glob}) aus datenträgerindividuellen Daten (ID) einschließlich einer individuellen Verifikationsfunktion (V_{card}) und einer Gültigkeit ($T_{gült}$) gebildet ist,

b) Mittel zur Verifikation des an das Terminal übergebenen Zertifikats im Terminal mit Hilfe einer im Terminal gespeicherten globalen Verifikationsfunktion (V_{glob}) und zur vorübergehenden Speicherung der datenträger-individuellen Daten (ID) und der individuellen Verifikationsfunktion (V_{card}),
c) Mittel zur Ableitung mindestens eines Schlüssels (K_{auth}; K_{red}) aus den datenträger-individuellen Daten (ID) und aus mindestens einem im Terminal gespeicherten übergeordneten Schlüssel (KM_{auth}; KM_{red}),
d) Mittel zum Datenaustausch zwischen dem Datenträger und dem Terminal einschließlich der Übergabe eines Datenänderungsbefehls des Terminals an den Datenträger mit einem Challenge-and—Response-Verfahren unter Verwendung des mindestens einen abgeleiteten Schlüssels (K_{auth}; K_{red}), das gleichzeitig eine Authentikation des Terminals gegenüber dem Datenträger realisiert,
e) Mittel zur Erstellung und Übergabe eines aus dem Datenänderungsbefehl resultierenden Buchungsdatensatzes in Form eines mit einer individuellen Signierfunktion (S_{card}) gebildeten Kryptogramms aus der Chipkarte an das Terminal und
f) Mittel zur Überprüfung des Kryptogramms mit Hilfe der individuellen Verifikationsfunktion (V_{card}) im Terminal und zum anschließenden Löschen der vorübergehend gespeicherten datenträger-individuellen Daten (ID, V_{card}) im Terminal."

Die unabhängigen Ansprüche 5 und 6 sind auf ein Verfahren zum gesicherten Lesen bzw. auf ein Verfahren zum gesicherten Lesen und Ändern von Daten gerichtet.

V. Es wird auf die folgenden Dokumente Bezug genommen:

B4: EMV '96, "Integrated Circuit Card Specification for Payment Systems", Version 3.0, June 30, 1996

B7: A. Beutelspacher, "Kryptologie", 5. Auflage, Seiten 90 bis 93, 100 bis 105, 113 bis 122, 136, 137 und 147.

VI. Die Beschwerdeführerin machte im Wesentlichen Folgendes geltend:

Anspruch 1 verstoße gegen die Vorschrift des Artikels 123(2) EPÜ. In der ursprünglich eingereichten Anmeldung seien keine Mittel, wie sie jetzt in dem vorliegenden Anspruch 1 erscheinen, offenbart worden. Zudem bleibe unklar, was und wo genau diese Mittel seien.

Bei den Merkmalen a), d) und f) des Anspruchs 1 fehlen konkrete Angaben zu den benutzten Schlüsselpaaren sowie dazu, dass die benutzten Schlüsselverfahren symmetrisch bzw. asymmetrisch seien und wie genau die gleichzeitige Authentikation des Terminals gegenüber dem Datenträger realisiert werde bzw. wie genau die Verifikation aussehe.

Weiter sei nur eine Übergabe des Buchungsdatensatzes zusammen mit dem daraus gebildeten Kryptogramm ursprünglich offenbart (vgl. insbesondere Ansprüche 8 bis 11). Merkmal e) des Anspruchs 1 offenbare jedoch nur die Übergabe des Kryptogramms.

Zudem beruhe der Gegenstand des Anspruchs 1 nicht auf einer erfinderischen Tätigkeit. Dokument B7 zeige bereits ein System zum gesicherten Lesen und Ändern von

Daten auf einer Chipkarte beruhend auf einem symmetrischen Challenge-and-Response-Verfahren und mit einem asymmetrischen Schlüsselverfahren für die Authentikation der Buchungsdaten zur Steigerung der Sicherheit. Zudem verweise B7 unmittelbar auf die Verwendung eines Zertifikats für die sichere Verwaltung des asymmetrischen Schlüsselpaares sowie auf die Ableitung des symmetrischen Schlüssels im Terminal aus Chipkartendaten mittels eines übergeordneten Schlüssels. Damit unterscheide sich das System nach Anspruch 1 vom Dokument B7 nur noch dadurch, dass das Zertifikat zudem aus einer Gültigkeit gebildet sei und dass die Mittel zur Überprüfung des Kryptogramms auch zum anschließenden Löschen der vorübergehend gespeicherten datenträger-individuellen Daten im Terminal ausgestaltet seien. Das erste Merkmal sei üblich und aus dem Dokument B4 bekannt. Das zweite Merkmal sei naheliegend, da es für den Fachmann offensichtlich sei, nicht benötigte Daten nach Abschluss des Geschäftsvorgangs zu löschen.

VII. Die Beschwerdegegnerin führte im Wesentlichen aus:

Anspruch 1 verstoße nicht gegen die Vorschrift des Artikels 123(2) EPÜ. In der ursprünglich eingereichten Anmeldung sei auch die Hardware-Seite des Systems offenbart und damit das Vorhandensein entsprechender Mittel. Die Zusammenstellung der Schlüsselpaare sowie der Aufschluss, ob die benutzten Schlüsselverfahren symmetrisch oder asymmetrisch seien, ergeben sich aus dem Anspruchskontext. Eine unzulässige Erweiterung des Anmeldungsgegenstandes liege somit nicht vor. Auch die gleichzeitige Authentikation des Terminals gegenüber dem Datenträger in Merkmal d) sowie die Verifikation in

Merkmal f) seien für den Fachmann nachvollziehbar und mit der ursprünglichen Offenbarung im Einklang.

Zudem beruhe der Gegenstand des Anspruchs 1 auf einer erfinderischen Tätigkeit. Die einzelnen Teile des Systems seien zwar an sich alle bekannt, nicht jedoch die beanspruchte vorteilhafte Kombination. Dokument B7 zeige insbesondere nicht die Übertragung der datenträger-individuellen Daten (ID) sowie des öffentlichen Schlüssels (V_{card}). Zudem sei die Gültigkeit in dem beanspruchten Zusammenhang in B7 nicht angesprochen. Weiter sei auch das abschließende Löschen der vorübergehend gespeicherten datenträger-individuellen Daten im Terminal im Stand der Technik nirgendwo angedeutet.

Entscheidungsgründe

1. Die Beschwerde ist zulässig.

2. *Änderungen*

2.1 Anspruch 1 basiert im Wesentlichen auf den ursprünglich eingereichten, auf ein System zum gesicherten Lesen und Ändern von Daten auf intelligenten Datenträgern gerichteten Ansprüchen 1 bis 3 und 5 sowie auf dem ursprünglich eingereichten, auf ein Verfahren zum gesicherten Bearbeiten von Daten auf intelligenten Datenträgern gerichteten Anspruch 11 und der Beschreibung des Beispieles gemäß Figur 2.

2.2 Nach Auffassung der Beschwerdeführerin sind die verschiedenen, in Anspruch 1 aufgenommenen Mittel so

nicht ursprünglich offenbart, so dass ein Verstoß gegen Artikel 123(2) EPÜ vorliege.

In der Anmeldung in der ursprünglich eingereichten Fassung wird jedoch nach Meinung der Kammer das beschriebene System auch als Hardware-System offenbart (vgl. Figur 1 und zugehörige Beschreibung), wobei implizit ist, dass für jeweils als System- bzw. Verfahrensschritt angegebene Merkmale entsprechende Hardware-Mittel zu dessen Durchführung vorhanden sind.

2.3 Auch in dem von der Beschwerdeführerin bemängelten Fehlen von Angaben, was und wo die Mittel sind, kann die Kammer keinen Verstoß gegen Artikel 123(2) EPÜ sehen, da diese Angaben sich, soweit erforderlich, aus der zu den jeweiligen Mitteln im Anspruch angegebenen Funktion ergeben.

2.4 Weiter sieht die Beschwerdeführerin in Merkmal e) des Anspruchs 1 eine unzulässige Erweiterung, da ihrer Meinung nach nur eine Übergabe des Buchungsdatensatzes zusammen mit dem daraus gebildeten Kryptogramm ursprünglich offenbart wurde (vgl. insbesondere Ansprüche 8 bis 11).

Da jedoch laut Figur 2 der Anmeldung nur das Kryptogramm übergeben wird, ist nach Meinung der Kammer auch diese Möglichkeit den ursprünglichen Anmeldungsunterlagen entnehmbar.

Was darüber hinaus das von der Beschwerdeführerin bemängelte Fehlen konkreter Angaben im Anspruch 1 anbelangt zu den benutzten Schlüsselpaaren, zu der symmetrischen bzw. asymmetrischen Beschaffenheit der

benutzten Schlüsselverfahren sowie zu der Verifikation in Merkmal f), ist der Kammer der Auffassung, dass diese Angaben sich implizit aus dem Anspruch 1 ergeben.

2.5 Der Schutzbereich wurde durch die Änderungen im Vergleich zu dem des Anspruchs 1 in der erteilten Fassung eingeschränkt, sodass sich keine Beanstandungen im Hinblick auf Artikel 123(3) EPÜ ergeben.

3. *Erfinderische Tätigkeit*

3.1 *Dokument B7*

3.1.1 Dokument B7, das den nächstliegenden Stand der Technik darstellt, zeigt ein System zum Einkaufen mit einer Chipkarte. Die Authentikation des Kunden bzw. seiner Chipkarte gegenüber dem Terminal des Kaufmannes wird entsprechend einem Protokoll zur Benutzerauthentikation durchgeführt (vgl. Seite 104, Zeilen 1 bis 4). Das Protokoll basiert auf der Challenge-and-Response-Methode unter Verwendung eines gemeinsamen geheimen Schlüssels, der sowohl der Chipkarte als auch dem Terminal zur Verfügung steht (vgl. Seite 102, letzter Absatz, Seite 103, erster Absatz und Seiten 90 bis 93, Abschnitt 4.2.2). Dabei erhält das Terminal von der Chipkarte die Identifikationsdaten und verschafft sich den dazugehörigen Schlüssel. Insbesondere kann dabei der Schlüssel von einem systemeinheitlichen "Globalschlüssel" abgeleitet werden (vgl. Seite 91, letzter Absatz).

Entgegen der von der Beschwerdegegnerin vertretenen Auffassung zeigt B7 somit die Übertragung der Identifikationsdaten der Chipkarte.

Zudem muss auch das Händlerterminal sich gegenüber der Chipkarte als authentisch ausweisen. Das diesbezügliche Protokoll läuft ebenfalls nach der Methode Challenge-and-Response ab (vgl. Seite 104, Zeilen 4 bis 11).

3.1.2 Weiter ist eine Authentikation der zum Kauf gehörenden Buchungsdaten ("elektronischer Scheck") erforderlich. Dieser Buchungsdatensatz ("Dokument"), der sich aus den von dem Händlerterminal zu der Chipkarte übermittelten Daten (Betrag etc.) ergibt (siehe auch Seite 105, Zeilen 5 bis 16), wird mittels einer Art MAC (Message Authentication Code) "unterschrieben" und dann von der Karte zum Händlerterminal geschickt (vgl. Seite 104, Zeilen 12 bis 14). Laut Dokument B7 ist "*Aber der Pferdefuß bei der Verwendung symmetrischer Algorithmen [..], dass jeder, der einen MAC prüfen kann, auch in der Lage ist, diesen fälschen zu können. (Er ändert einfach das Dokument und berechnet mit Hilfe des geheimen Schlüssels den zugehörigen neuen MAC). Hier würden sich asymmetrischen Signaturschemata (siehe Kapitel 5) als eleganteste Lösung anbieten*" (vgl. Seite 104, Zeilen 12 bis Seite 105, Zeile 2).

Das asymmetrische Signaturschema wird gemäß Dokument B7 auf folgende Weise realisiert (vgl. Kapitel 5, insbesondere Seite 119, Abschnitt 5.2 und Seite 120, Figur 5.4):
Die Nachricht wird vom Sender mit dem geheimen (privaten) Schlüssel (E) eines Schlüsselpaares (E, D) eines asymmetrischen Kryptosystems verschlüsselt und die so entstandene Unterschrift wird (mit oder ohne Nachricht) versendet; der Empfänger verifiziert die Unterschrift, indem er sie mit dem öffentlichen Schlüssel D des

Schlüsselpaares (E, D) entschlüsselt.

Damit ergibt sich unmittelbar aus Dokument B7 die Lehre, bei der obenstehenden Authentikation des zum Kauf gehörenden Buchungsdatensatzes, diesen mit dem geheimen (privaten) Schlüssel eines Schlüsselpaares eines asymmetrischen Kryptosystems zu verschlüsseln und die so entstandene Unterschrift zu versenden. Die Unterschrift wird anschließend vom Empfänger verifiziert, indem er sie mit dem öffentlichen Schlüssel des Schlüsselpaares entschlüsselt.

3.1.3 Schließlich wird in Dokument B7 darauf hingewiesen, dass asymmetrische Algorithmen den Nachteil haben, ein gewisses Schlüsselmanagement zu benötigen (vgl. Seite 118, Zeilen 30 bis 38). Ein Missbrauch könnte nämlich darin bestehen, dass ein nicht authentisches Schlüsselpaar benutzt wird. Nach Dokument B7 kann man einem solchen Missbrauch entkommen, "*indem man eine trickreiche Schlüsselverwaltung durchführt, die gewährleistet, dass die Schlüssel "authentisch" sind. Dies wird in Übungsaufgabe 15 erläutert*" (Seite 119, Zeilen 1 bis 3).

Gemäß dieser Übungsaufgabe geht man um diesem Missbrauch zu begegnen wie folgt vor:
Ein öffentlicher Schlüssel eines Teilnehmers ist nur dann gültig, wenn er und der Name des Teilnehmers von einer vertrauenswürdigen (zentralen) Stelle CA (Certification Authority) zertifiziert ist. Dazu signiert CA den Schlüssel E und den Namen des Teilnehmers mit ihrem geheimen Schlüssel. Diese Signatur wird zusammen mit dem öffentlichen Schlüssel E gespeichert. Bevor ein (anderer) Teilnehmer den

Schlüssel E benutzt, muss er die elektronische Unterschrift mit Hilfe des öffentlichen Schlüssels von CA verifizieren (vgl. Seite 147, Aufgabe 15).

Für die obengenannte Authentikation des zu dem Kauf gehörenden Buchungsdatensatzes bedeutet dies, dass der öffentliche Schlüssel des Schlüsselpaares des asymmetrischen Schlüsselverfahrens zusammen mit den Identifikationsdaten der Chipkarte von einer vertrauenswürdigen (zentralen) Stelle CA (Certification Authority) mit ihrem geheimen Schlüssel signiert wird und dass, bevor das Händlerterminal den öffentlichen Schlüssel des asymmetrischen Schlüsselverfahrens benutzt, es die elektronische Unterschrift mit Hilfe des öffentlichen Schlüssels von CA verifiziert.

Dies setzt im Übrigen voraus, dass entgegen der Auffassung der Beschwerdegegnerin eine Übertragung des öffentlichen Schlüssels dieses Schlüsselpaares zum Händlerterminal stattfindet.

3.2 *Anspruch 1*

3.2.1 Konkret in der Terminologie des vorliegenden Anspruchs 1 zeigt Dokument B7 folglich ein System zum gesicherten Lesen und Ändern von Daten auf intelligenten Datenträgern, insbesondere IC-Karten ("Chipkarte"), mit Terminals ("Händlerterminal"), die einer übergeordneten Zentrale (die für die Abwicklung der Buchung zuständige Bank (vgl. Seite 104, Bild 4.17 und zugehörige Beschreibung) bzw. die obengenannte zentrale Stelle CA) zugeordnet und mit zur temporären Kommunikation mit den Datenträgern geeigneten Schnittstellen (zwangsläufig

vorhanden für den Datenaustausch zwischen Chipkarte und Händlerterminal in B7) ausgestattet sind.

3.2.2 Auf jedem Datenträger ("Chipkarte") ist neben der auszulesenden oder zu ändernden Information (der zu dem Kauf gehörende Buchungsdatensatz) und einer Identifikationsinformation (z. B. der Name des Kunden bzw. des Karteninhabers) ein Schlüssel gespeichert, der auch den Terminals zur Authentikation des jeweiligen Datenträgers nach einem symmetrischen Schlüsselverfahren zur Verfügung steht (der obengenannte symmetrische Schlüssel für die Authentikation der Chipkarte gegenüber dem Terminal, vgl. Punkt 3.1.1).

3.2.3 Weiter weist das aus B7 bekannte System ein auf dem Datenträger zur Übergabe an das Terminal gespeichertes Zertifikat (das obengenannte, von der zentralen Stelle CA (Certification Authority) abgegebene Kryptogramm) auf, das mit Hilfe einer zur Zertifizierung der im System zu verwendenden Datenträger dienenden globalen Signierfunktion (der geheime Schlüssel der zentralen Stelle CA) aus datenträger-individuellen Daten (z. B. der Name des Teilnehmers) einschließlich einer individuellen Verifikationsfunktion (der obengenannte öffentliche Schlüssel des asymmetrischen Schlüsselverfahrens, vgl. Punkt 3.1.2) gebildet ist.

3.2.4 Zudem weist das aus B7 bekannte System Mittel auf zur Verifikation des an das Terminal übergebenen Zertifikats im Terminal mit Hilfe einer im Terminal gespeicherten globalen Verifikationsfunktion (die obenerwähnte Verifizierung des Kryptogramms mittels des öffentlichen Schlüssels der zentralen Stelle CA, vgl. Punkt 3.1.3) und zur vorübergehenden Speicherung der datenträger-

individuellen Daten und der individuellen Verifikationsfunktion (der öffentliche Schlüssel des asymmetrischen Schlüsselverfahrens) (eine Speicherung muss auch gemäß B7 zwangsläufig stattfinden, da diese Daten anschließend benötigt werden).

3.2.5 Darüber hinaus zeigt B7, wie oben dargelegt (vgl. Punkt 3.1.1), die Möglichkeit auf, Mittel vorzusehen zur Ableitung mindestens eines Schlüssels aus den datenträger-individuellen Daten und aus mindestens einem im Terminal gespeicherten übergeordneten Schlüssel ("Globalschlüssel").

3.2.6 Weiter zeigt B7 Mittel zum Datenaustausch zwischen dem Datenträger und dem Terminal einschließlich der Übergabe eines Datenänderungsbefehls ("Buchungsdaten") des Terminals an den Datenträger mit einem Challenge-and-Response-Verfahren unter Verwendung des mindestens einen abgeleiteten Schlüssels (der symmetrische Schlüssel für die Authentikation, vgl. Punkt 3.1.1), das gleichzeitig eine Authentikation des Terminals gegenüber dem Datenträger realisiert (das obenerwähnte Challenge-and-Response-Verfahren bewirkt auch eine Authentikation des Händlerterminals gegenüber der Chipkarte, vgl. Punkt 3.1.1, letzter Absatz).

3.2.7 Darüber hinaus umfasst die Lehre des Dokuments B7 Mittel zur Erstellung und Übergabe eines aus dem Datenänderungsbefehl resultierenden Buchungsdatensatzes in Form eines mit einer individuellen Signierfunktion (der obengenannte private Schlüssel des asymmetrischen Schlüsselverfahrens, vgl. Punkt 3.1.2) gebildeten Kryptogramms aus der Chipkarte an das Terminal.

3.2.8 Schließlich zeigt B7 Mittel zur Überprüfung des Kryptogramms mit Hilfe der individuellen Verifikationsfunktion (der öffentliche Schlüssel des asymmetrischen Schlüsselverfahrens) im Terminal.

3.3 Nicht dem Dokument B7 entnehmbar sind die Merkmale des Anspruchs 1, dass
(I) das Zertifikat zudem aus einer Gültigkeit gebildet ist, und dass
(II) die Mittel zur Überprüfung des Kryptogramms zum anschließenden Löschen der vorübergehend gespeicherten datenträger-individuellen Daten im Terminal ausgestaltet sind.

Der Gegenstand des Anspruchs 1 ist folglich neu gegenüber Dokument B7. Die Neuheit wurde im Übrigen im vorliegenden Fall auch nicht bestritten.

3.4 Diese beiden Merkmale I und II des Anspruchs 1 stellen voneinander unabhängige Maßnahmen dar, die keinen Synergieeffekt aufweisen, und können somit bei der Beurteilung der erfinderischen Tätigkeit getrennt beurteilt werden.

Die Berücksichtigung einer Gültigkeit bei der Bildung eines Zertifikats (Merkmal I) ermöglicht die Beschränkung der Gültigkeitsdauer des Zertifikats. Die sich hieraus ergebende objektive Teilaufgabe, eine zweckmäßige und sichere Verwaltung der Zertifikate, ist für den Fachmann bei den vorliegenden Systemen naheliegend. Zudem ist die beanspruchte Lösung eine für Zertifikate übliche Maßnahme, die als solche aus dem Dokument B4 bekannt ist (vgl. Seite IV-12, Tabelle IV-6, vierte Zeile). Der Fachmann würde somit diese Maßnahme

ohne erfinderisches Zutun in einem System nach Dokument B7 vorsehen.

Das Löschen der vorübergehend gespeicherten datenträger-individuellen Daten im Terminal (Merkmal II) ermöglicht eine zweckmäßige Datenverwaltung im Terminal. Die sich hieraus ergebende objektive Teilaufgabe, eine angebrachte Datenverwaltung im Terminal zu bieten, ist für den Fachmann naheliegend, insbesondere in Anbetracht des endlichen im Terminal zur Verfügung stehenden Speicherplatzes. Zudem ist es für den Fachmann unmittelbar ersichtlich, dass diese Daten nach Abschluss des Geschäftsvorganges nicht mehr weiter gebraucht werden und somit nur Speicherplatz im Terminal wegnehmen.

Der Gegenstand des Anspruchs 1 beruht somit nicht auf einer erfinderischen Tätigkeit im Sinne von Artikel 56 EPÜ 1973.

Entscheidungsformel

Aus diesen Gründen wird entschieden:

1. Die angefochtene Entscheidung wird aufgehoben.

2. Das Patent wird widerrufen.

Der Geschäftsstellenbeamte: Der Vorsitzende:

S. Sánchez Chiquero G. Eliasson