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 10. Juni 2010

Beschwerde-Aktenzeichen: T 1233/07 - 3.4.03

Anmeldenummer: 98916888.5

Veröffentlichungsnummer: 0970449

IPC: G07F 7/10

Verfahrenssprache: DE

Bezeichnung der Erfindung:
Tragbarer Datenträger und Verfahren zu dessen kryptographisch gesicherten Benutzung mit austauschbaren kryptographischen Schlüsseln

Patentinhaber:
Deutsche Telekom AG

Einsprechender:
GIESECKE & DEVRIENT GmbH

Stichwort:
-

Relevante Rechtsnormen:
-

Relevante Rechtsnormen (EPÜ 1973):
EPÜ Art. 54(1)(2)

Schlagwort:
"Neuheit (nein)"

Zitierte Entscheidungen:
-

Orientierungssatz:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Aktenzeichen: T 1233/07 - 3.4.03

E N T S C H E I D U N G
der Technischen Beschwerdekammer 3.4.03
vom 10. Juni 2010

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

Vertreter:
-

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. 0970449 in geändertem Umfang, zur Post gegeben am 3. Juli 2007.

Zusammensetzung der Kammer:

Vorsitzender: G. Eliasson
Mitglieder: R. Q. Bekkering
T. Bokor

Sachverhalt und Anträge

I. Die Beschwerde richtet sich gegen die Zwischenentscheidung der Einspruchsabteilung, das Patent Nr. 0 970 449 in geändertem Umfang aufrechtzuerhalten. Einzige Beschwerdeführerin ist die Einsprechende.

II. Die Patentinhaberin und Beschwerdegegnerin nahm, wie vorab angekündigt, nicht an der mündlichen Verhandlung vor der Beschwerdekammer teil.

III. Die Beschwerdeführerin beantragte, die angefochtene Entscheidung aufzuheben und das Patent zu widerrufen.

IV. Die Beschwerdegegnerin hat schriftlich beantragt, die Beschwerde zurückzuweisen und das Patent in geändertem Umfang gemäß der Zwischenentscheidung der Einspruchsabteilung aufrechtzuerhalten.

V. Anspruch 1 lautet:

"*Tragbarer Datenträger, insbesondere Chipkarte, zum Speichern von Daten in Form von Datensätzen, wobei zur Absicherung des Schreibens und Lesens der Datensätze kryptographische Schlüssel (32, 33) und eine Reihe von Schlüsseln (32, 33) für den jeweiligen Verwendungszweck auf dem Datenträger (7) gespeichert sind, dadurch gekennzeichnet, daß Mittel (30) zur Unbrauchbarmachung von Schlüsseln (32, 33) im Datenträger (7) vorgesehen sind.*"

Anspruch 5 lautet:

"*Verfahren zur Benutzung eines Datenträgers, insbesondere Chipkarte, zum Speichern von Daten in Form von Datensätzen, wobei zur Absicherung des Schreibens und Lesens der Datensätze kryptographische Schlüssel (32, 33) und eine Reihe von Schlüsseln (32, 33) für den jeweiligen Verwendungszweck auf dem Datenträger (7) gespeichert sind, wobei Mittel (30) zur Unbrauchbarmachung von Schlüsseln (32, 33) im Datenträger (7) vorgesehen sind und wobei in jedem Datensatz, insbesondere Berechtigungsdatensatz, Speicherplatz vorgesehen ist, worin ein Identifikationsmerkmal (42) desjenigen Schlüssels (33) speicherbar ist, mit dem der Datensatz zuletzt geschrieben wurde, dadurch gekennzeichnet, daß vor jeder Benutzung eines Schlüssels (33) zum Schreiben oder Lesen von Daten geprüft wird, ob der Schlüssel (33) älter ist als derjenige, dessen Identifikationsmerkmal (42) auf dem Datenträger gespeichert ist und daß bei positivem Ergebnis dieser Prüfung die Benutzung des Schlüssels (33) durch im Datenträger vorgesehene Mittel abgelehnt wird.*"

VI. Es wird auf das folgende Dokument Bezug genommen:

E2: W. Rankl, W. Effing, "Handbuch der Chipkarten", Carl Hanser Verlag, München-Wien, 1995, Seiten 205 bis 207 (zitiert in der Einspruchsschrift) und 273 bis 276 (ergänzend von der Kammer zitiert).

VII. Die Beschwerdeführerin hat im Wesentlichen Folgendes vorgetragen:

Wie in der Entscheidung dargelegt, sei aus der Entgegenhaltung E2 bekannt, dass Nutzdaten auf der Speicherkarte gespeichert seien, kryptographische Schlüssel für die gesicherte Datenübertragung verwendet werden und Mittel zur Unbrauchbarmachung von Schlüsseln im Datenträger vorgesehen seien, gemäß Anspruch 1 des Streitpatents.

Die Einspruchsabteilung erkenne zwar an, dass in Kapitel 8.3.5 der Entgegenhaltung E2 offenbart sei, dass Schlüssel mit Schlüsselnummer, Verwendungszweck und Versionsnummer auf der Karte gespeichert seien und mit Hilfe dieser Daten adressiert werden, sie sehe es jedoch nicht als offenbart oder nahegelegt an, dass gleichzeitig mehrere Schlüssel für den gleichen Verwendungszweck auf der Karte gespeichert seien.

Jedoch müsste, der Interpretation des Patentinhabers bzw. der Einspruchsabteilung der Entgegenhaltung E2 zufolge, wonach nur eine Schlüsselversion in der Karte gespeichert sei, bei jedem Wechsel der Schlüsselversion die Chipkarte in eine gesicherte Umgebung gebracht werden oder zumindest ein gesicherter Datenaustausch ermöglicht werden. Dies sei nicht nur aufwendig sondern bei vielen Einsatzgebieten nicht möglich. Der Fachmann könne deshalb aus der Formulierung in E2, 8.3.5 nur den Schluss ziehen, dass die "Adressierung" mit Versionsnummer nur bedeuten könne, dass mehrere Versionen in der Karte gespeichert seien, so dass Anspruch 1 nahegelegt sei.

Die gegenüber Anspruch 1 im Anspruch 5 zusätzlich aufgeführten Merkmale seien, soweit sie eine Einschränkung darstellen, ebenfalls aus E2 bekannt. Insbesondere seien die Merkmale des kennzeichnenden Teils des Anspruchs 5 wiederum aus der Entgegenhaltung E2 bekannt. Dort werde auf S. 206, Abs. 2 und 3 unter Kap. 8.3.3 beschrieben, dass im Regelfall für die Lebensdauer der Chipkarte mehrere Schlüsselgenerationen vorgesehen seien. Die Umschaltung zwischen den Schlüsselgenerationen könne in einem festen oder variablen Zeitraster erfolgen. Bei mehreren möglichen Schlüsselversionen bzw. -generationen müsse demnach vor jeder Benutzung des Schlüssels geprüft werden, ob der Schlüssel älter sei als derjenige, dessen Identifikationsmerkmal (z.B. Versionsnummer) auf dem Datenträger gespeichert sei. Des Weiteren werde in E2 die Umschaltung von einer Schlüsselgeneration auf die nächste aus Sicherheitsgründen durchgeführt, sodass zwangsläufig die Benutzung älterer Schlüssel nicht erlaubt sei.

VIII. Die Beschwerdegegnerin hat im Wesentlichen wie folgt argumentiert:

Das Patent beschäftige sich mit Chipkarten, welche Berechtigungen in elektronischer Form enthalten. Derartige Chipkarten benötigen keine Individualisierung, d.h. es sind keine persönlichen Daten gespeichert. Deshalb seien bei diesen Chipkarten außer der Absicherung des Schreibens und Lesens der die Berechtigungen darstellenden Daten keine Sicherungsmaßnahmen erforderlich.

Im Gegensatz dazu betreffe die Druckschrift E2 die Verwaltung von Schlüsseln für Signaturen, gesicherte Datenübertragung, Authentisierung und Verschlüsselung. Derartige Systeme erfordern ein relativ komplexes Schlüsselmanagement, wie es in E2 beschrieben werde.

Da bei den erfindungsgemäßen Chipkarten ein komplexes Schlüsselmanagement gemäß E2 nicht erforderlich sei, würde der Fachmann E2 nicht eingehend daraufhin überprüfen, ob aus E2 eventuell Lehren für die Lösung der erfindungsgemäßen Aufgabe abgeleitet werden können.

Darüber hinaus sei aus E2 nicht bekannt, eine Reihe von Schlüsseln für den jeweiligen Verwendungszweck auf der Chipkarte zu speichern. Es sei durchaus möglich, nur jeweils pro Verwendungszweck eine Schlüsselversion zu speichern. Gemäß E2 (letzter Absatz vor Bild 8.7) werde, wenn die Chipkarte von einem Terminal, der auf eine neue Schlüsselversion umgestellt sei, einen Sperrvermerk für den Schlüssel erhalte, verhindert, dass dieser Schlüssel bzw. die Chipkarte im Zusammenhang mit einem Terminal, der noch nicht auf eine neue Schlüsselnummer umgestellt sei, benutzt werde. Im Gegensatz zur Erfindung werde jedoch die derartige Chipkarte unbenutzbar.

Im Übrigen handele es sich bei den übrigen beanspruchten Merkmalen um eine Kombination, die bereits eine gewisse Auswahl darstelle, die in dieser Form in E2 nicht offenbart sei.

Der Gegenstand des Anspruchs 1 sei somit weder dem Dokument E2 entnehmbar noch sonst nahegelegt und somit neu und erfinderisch.

Was Anspruch 5 anbelange, seien die Merkmale, wonach in jedem Datensatz, insbesondere Berechtigungsdatensatz, Speicherplatz vorgesehen ist, worin ein Identifikationsmerkmal desjenigen Schlüssels speicherbar ist, mit dem der Datensatz zuletzt geschrieben wurde, und vor jeder Benutzung eines Schlüssels zum Schreiben oder Lesen von Daten geprüft wird, ob der Schlüssel älter ist als derjenige, dessen Identifikationsmerkmal (42) auf dem Datenträger gespeichert ist, in keiner Weise der Entgegenhaltung E2 entnehmbar, so dass hier auch nicht nur andeutungsweise von einem Mangel eines erfinderischen Schrittes ausgegangen werden könne.

Damit sei auch der Gegenstand des Anspruchs 5 neu und beruhe auf einer erfinderischen Tätigkeit.

Entscheidungsgründe

1. Die Beschwerde ist zulässig.

2. *Anspruch 1*

2.1 Das Merkmal in Anspruch 1 "*wobei zur Absicherung des Schreibens und Lesens der Datensätze kryptographische Schlüssel (32, 33) und eine Reihe von Schlüsseln (32, 33) für den jeweiligen Verwendungszweck auf dem Datenträger (7) gespeichert sind*" ist offenbar dahingehend zu verstehen, dass eine Reihe von kryptographischen Schlüsseln für den jeweiligen Verwendungszweck auf dem Datenträger gespeichert sind, einschließlich einer Reihe von kryptographischen Schlüsseln zur Absicherung des Schreibens und Lesens der Datensätze (vgl. auch

Anspruch 1 in der ursprünglich eingereichten Fassung; Beschreibung, Seite 6, zweiter Absatz und Figur 3).

2.2 *Neuheit*

2.2.1 Dokument E2, ein Handbuch auf dem Gebiet der Chipkarten, zeigt einen tragbaren Datenträger, insbesondere eine Chipkarte, zum Speichern von Daten in Form von Datensätzen. Dabei sind zur Absicherung des Schreibens und Lesens der Datensätze kryptographische Schlüssel auf dem Datenträger gespeichert (vgl. Seite 205, Kapitel 8.3 zweiter Absatz; Seite 205, Kapitel 8.3.2; Seite 207, Kapitel 8.3.5, erster Absatz und Bild 8.7; Seite 274, Kapitel "Daten").

Entgegen der Meinung der Beschwerdegegnerin betrifft E2 auch eine "einfache" Verschlüsselung von Daten in Form von Datensätzen zur Absicherung des Schreibens und Lesens der Datensätze auf der Chipkarte, wie in dem vorliegenden Patent.

2.2.2 In der angefochtenen Entscheidung wird argumentiert, dass in E2 nicht eindeutig offenbart sei, dass mehrere Schlüssel für den gleichen Verwendungszweck auf der Karte gespeichert seien (Gründe, Punkt 3.1). Zum Einen sei es durchaus von Nutzen, wenn die Karte nur einen einzigen Schlüssel pro Verwendungszweck enthalte (vgl. Gründe, Punkt 3.3) und zum Anderen sei es nicht zwingend, dass alle Schlüsselgenerationen auf der Karte gespeichert seien, da sie auch nach Bedarf generiert werden könnten (vgl. Gründe, Punkt 4.1).

Wie jedoch bereits in Absatz 8.3.3 in E2 zum Prinzip der Schlüsselversionen angeführt wird, besitzen alle

modernen Systeme die Möglichkeit, auf neue Schlüsselgenerationen weiterzuschalten, um bei Kompromittierung eines Schlüssels ein Austauschen der Karten zu vermeiden. Nach E2 kann das Umschalten im schlimmsten Fall durch die Kompromittierung eines Schlüssels erzwungen werden oder routinemäßig in einem festen oder variablen Zeitraster geschehen. Das Ergebnis ist laut E2, dass alle Schlüssel im System durch neue ausgetauscht worden sind, ohne dass eine Rückrufaktion für die Chipkarten notwendig geworden wäre.

Das Argument der Beschwerdegegnerin, dass nur ein einziger Schlüssel pro Verwendungszweck auf der Karte gespeichert sei, ist somit nicht überzeugend, da in diesem Fall, bei Kompromittierung eines Schlüssels, eine Rückrufaktion für die Chipkarten, die eben laut E2 vermieden wird, notwendig wäre.

Zu dem Argument in der angefochtenen Entscheidung, dass es nicht zwingend sei, dass alle Schlüsselgenerationen auf der Karte gespeichert seien, da sie auch nach Bedarf generiert werden könnten, ist anzumerken, dass es nicht ersichtlich ist, wie dies in sicherer Weise geschehen sollte. Dokument E2 enthält auf jeden Fall keinerlei Hinweis auf ein solches Vorgehen.

Ergänzend wird außerdem in E2 (vgl. Kapitel 12.1.2) zu diesem Thema (vgl. Absatz "Schlüsselmanagement") noch dargelegt, dass, um auch den Fall der Kompromittierung des Hauptschlüssels abzusichern, wobei aber ein Austausch der Karten wirtschaftlich indiskutabel wäre, mehrere Generationen von kartenindividuellen Schlüsseln in die Karte eingebracht werden können, sodass

gegebenenfalls auf eine neue Schlüsselgeneration umgeschaltet werden kann.

Zudem wird in E2 auf Seite 274, sechster Absatz sowie auch auf Seite 205, Absatz 8.3 darauf hingewiesen, dass die Anwendung des Prinzips der Schlüsselversionen dazu führt, dass die Zahl der Schlüssel und damit der Speicherbedarf zunimmt, woraus sich ergibt, dass mehrere Schlüsselgenerationen auf der Karte gespeichert sind.

Damit ist es nach Auffassung der Kammer aus E2 bekannt, dass eine Reihe von Schlüsseln für den jeweiligen Verwendungszweck auf dem Datenträger gespeichert ist, wie von Anspruch 1 vorgeschrieben.

2.2.3 Schließlich zeigt E2 auch, dass der Schlüssel in der Chipkarte mit einem Sperrvermerk ausgestattet werden kann, der aktiviert wird, sobald ein neuer Schlüssel mit gleicher Schlüsselnummer angesprochen wird, wodurch die Wiederverwendung alter Schlüsselversionen im System verhindert wird (vgl. Seite 207, dritter Absatz und Bild 8.7).

2.2.4 Entgegen dem Argument der Beschwerdegegnerin, bei den beanspruchten Merkmalen handele es sich um eine Kombination, die bereits eine gewisse Auswahl darstelle, die in dieser Form in E2 nicht offenbart sei, ist festzustellen, dass vielmehr in E2 verschiedene Ausgestaltungen der Chipkarte, insbesondere mit verschiedenen kryptographischen Funktionen der Schlüssel, offenbart sind, wobei der Anspruchsgegenstand eben einer dieser Ausgestaltungen entspricht. Damit zeigt nach Auffassung der Kammer E2 bereits die Kombination dieser Merkmale und nicht nur die Einzelmerkmale.

2.2.5 Der Gegenstand des Anspruchs 1 ist somit nicht neu gegenüber dem Dokument E2 (Artikel 54(1) und (2) EPÜ 1973).

3. *Anspruch 5*

3.1 *Neuheit*

Die Merkmale des Anspruchs 5, die den Merkmalen des Anspruchs 1 entsprechen, sind wie vorstehend dargelegt aus dem Dokument E2 bekannt.

Zudem wird in E2 ausgeführt, dass die Verwendung mehrerer Schlüsselgenerationen im System dazu dient, die Sicherheit zu gewährleisten, auch wenn z.B. der Hauptschlüssel in den Terminals kompromittiert ist. Nach der Umschaltung auf eine neue Schlüsselgeneration (neuer Hauptschlüssel in den Terminals und neuer Schlüssel in der Karte) ist die Verwendung der älteren, kompromittierten Schlüsselgeneration zu unterbinden. Nach E2 ist dies mit einem auf der Karte gespeicherten Sperrvermerk zu dem alten Schlüssel realisierbar, der aktiviert wird, sobald ein neuer Schlüssel angesprochen wird (Seite 207, dritter Absatz und Bild 8.7).

Damit ist aus den auf der Karte gespeicherten jeweiligen Sperrvermerken der Schlüsselversionen ableitbar, welcher Schlüssel zuletzt angesprochen wurde und für das Lesen und Schreiben von Daten eingesetzt wurde. Damit stellen die Sperrvermerke aus E2 ein Identifikationsmerkmal im Sinne des Anspruchs 5 dar. Insbesondere ist damit gemäß E2 im jedem Datensatz Speicherplatz vorgesehen, worin ein Identifikationsmerkmal desjenigen Schlüssels

speicherbar ist, mit dem der Datensatz zuletzt geschrieben wurde, wie von Anspruch 5 vorgeschrieben.

Würde man nun mit einem älteren Schlüssel versuchen, Daten auf der Karte zu lesen oder zu schreiben, würde dies nach E2 aufgrund der vorhandenen, in der Karte gespeicherten Sperrvermerke durch entsprechende Mittel abgelehnt werden. Dieser Vorgang entspricht den Merkmalen gemäß dem kennzeichnenden Teil des Anspruchs 5.

Der Gegenstand des Anspruchs 5 ist somit ebenfalls nicht neu gegenüber dem Dokument E2 (Artikel 54(1) und (2) EPÜ 1973).

4. Aus den vorstehenden Gründen ist der Antrag der Beschwerdegegnerin nicht gewährbar.

Entscheidungsformel

Aus diesen Gründen wird entschieden:

1. Die angefochtene Entscheidung wird aufgehoben.

2. Das Patent wird widerrufen.

Die Geschäftsstellenbeamtin: Der Vorsitzende:

S. Sánchez Chiquero G. Eliasson