BUNDESPATENTGERICHT

20 W (pat) 332/02

(Aktenzeichen)

Verkündet am
22. September 2003
…

B E S C H L U S S

In der Einspruchssache

…

betreffend das Patent 197 18 547

…

hat der 20. Senat (Technischer Beschwerdesenat) des Bundespatentgerichts auf die mündliche Verhandlung vom 22. September 2003 durch den Vorsitzenden Richter Dipl.-Phys. Dr. Anders sowie den Richter Dipl.-Ing. Obermayer, die Richterin Martens und den Richter Dipl.-Phys. Dr. Zehendner

beschlossen:

Das Patent wird widerrufen.

G r ü n d e

I

Das mit dem Einspruch angegriffene Patent 197 18 547 betrifft ein

"System zum gesicherten Lesen und Ändern von Daten auf intelligenten Datenträgern".

Die Einsprechende führt aus, der Gegenstand des Patents beruhe nicht auf erfinderischer Tätigkeit.

Sie beantragt,

das Patent zu widerrufen.

Die Patentinhaberin stellt den Antrag,

das Patent in vollem Umfang aufrechtzuerhalten.

Der erteilte 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:

- 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}) gebildet ist,
- Mittel zur Verifikation des Zertifikats im Terminal mit Hilfe einer im Terminal gespeicherten globalen Verifikationsfunktion (V_{glob}) und zur vorübergehenden Speicherung der datenträgerindividuellen Daten (ID) und der individuellen Verifikationsfunktion (V_{card}),
- Mittel zur Authentikation des Datenträgers gegenüber dem benutzten Terminal mit einem symmetrischen Schlüsselverfahren,
- Mittel zur Authentikation des Terminals gegenüber dem Datenträger und Übergabe eines Auslesebefehls an den Datenträger mit Hilfe des symmetrischen Schlüsselverfahrens,

- Mittel zur Übergabe der auszulesenden Daten in Form eines mit einer individuellen Signierfunktion (S_{card}) gebildeten Kryptogramms an das Terminal und
- Mittel zur Überprüfung des Kryptogramms mit Hilfe der individuellen Verifikationsfunktion (V_{card}) im Terminal und zum anschließenden Löschen der vorübergehend gespeicherten datenträgerindividuellen Daten (ID, V_{card}) im Terminal."

In der mündlichen Verhandlung werden ua Stellen aus folgenden Fachbüchern erörtert:

W. Rankl, W. Effing, "Handbuch der Chipkarten", 2. Aufl., 1996, Hanser-Verlag (D3) Beutelspacher, Kersten, Pfau, "Chipkarten als Sicherheitswerkzeug", Springer-Verlag, 1991 (D4).

II

Das Patent ist nicht rechtsbeständig, sein Gegenstand nach den §§ 1 und 4 PatG nicht patentfähig. Er ist dem Fachmann durch (D4) nahegelegt.

Als Fachmann gilt hier ein Elektroingenieur oder Informatiker mit Fachhochschulabschluß, der mit dem Aufbau und der Funktionsweise von Chipkarten vertraut ist. Bei der Vielfalt von Anwendungsmöglichkeiten dieser intelligenten Datenträger ist er namentlich damit befaßt, sich umfassend Gedanken über ihren möglichst sicheren Einsatz zu machen.

Hierzu zeigt ihm (D4) als Möglichkeit zur gegenseitigen Authentifizierung elektronischer Partner in einem Kommunikationssystem die gegenseitige Authentifizierung mit symmetrischen Algorithmen. Dabei wird zwar der Fall betrachtet, daß der eine Partner eine Chipkarte und der andere ein Rechner ist (S 61 bis 63

Abschn 4.1.2.1). Auf der Chipkarte ist neben einer Identifikationsinformation CID ein Schlüssel K_C gespeichert, der auch dem Rechner als Schlüssel K_R für die Prüfprozedur zur Verfügung steht (Bild 4.2).

Als Gegenüber für den intelligenten Datenträger hat der Fachmann aber nicht nur einen Rechner im Auge; auch ein Terminal ist als Partner der Chipkarte vorstellbar, wie dies im übrigen anhand der Druckschrift (D3) für das in Rede stehende Verschlüsselungsverfahren belegt ist (S 272, 273 Abschn 8.2.2). Als Chipkarten-Terminal kommen dabei tragbare und stationäre Geräte infrage, wobei stationäre Terminals einem übergeordneten Rechnersystem zugeordnet sein können (S 338).

Dies deckt sich auch mit den Ausführungen in (D4), da bei der Anwendung der Chipkarte als Werkzeug im elektronischen Zahlungsverkehr neben der Chipkarte ein Händlerterminal, eine Autorisierungszentrale und Banken als Partner genannt sind (S 99 Punkt 2 iVm S 100 Abschn 5.2).

Damit ergeben sich aus (D4) die Merkmale im Oberbegriff und das 3. und 4. kennzeichnende Merkmal.

Es liegt nahe, bei der Verwendung der Chipkarte als "elektronische Geldbörse" nicht nur zu überprüfen, ob Chipkarte und Terminal gegenseitig berechtigt sind oder nicht. Dem Fachmann liegt an möglichst fälschungssicherem Zahlungsverkehr. Hierzu benutzt er zusätzlich noch ein asymmetrisches Signaturschema. Denn bei abgeschlossener gegenseitiger symmetrischer Authentisierung wissen zwar das Terminal und die Chipkarte, daß der jeweils andere Partner vertrauenswürdig ist. Gleichwohl ist nicht sichergestellt, daß dann der von der Chipkarte zum Terminal übertragene Buchungsdatensatz auch unverfälscht ist. Wenn man die Daten der Chipkarte verändert, so liegt daran, die Veränderungen der Daten zu dokumentieren, damit später eine Rückverfolgung möglich ist. Hierzu ist die elektronische Unterschrift das geeignete Mittel ((D4) S 125, 126 Abschn 5.4.2). Dies

gilt nicht nur für den Einsatz der Chipkarte als Dokument ((D4) S 99 Punkt 3), sondern auch als elektronisches Zahlungsmittel ((D4) S 99 Punkt 2), wie (D3) belegt (S 370 Abs 1).

Ein zusätzliches asymmetrisches Authentisierungsverfahren bedeutet vermehrten Schutz ((D3) S 273 le Abs Satz 1). Die Datenintegrität und –authentizität der zu verändernden Geldbeträge sind dabei durch den Mechanismus der elektronischen Unterschrift gesichert ((D 4) S 70, 71). Hierzu werden – entsprechend dem vorletzten und dem letzten kennzeichnenden Merkmal - die von der Karte auszusendenden Daten M in Form eines mit einer individuellen Signierfunktion s_{DA} gebildeten Kryptogramms an das Terminal übermittelt und dort mit Hilfe eines öffentlichen Schlüssels E_A mittels der Funktion v_{EA} verifiziert (Bild 4.8).

Dabei bietet es sich aber für den Fachmann an, nicht mit einem öffentlichen Schlüssel E_A zu arbeiten, sondern mit einem zum jeweiligen Terminal gehörenden öffentlichen Schlüssel E_{ID}: Durch ein Zertifikat stellt man eine Verbindung zwischen der Identität des Kartenbenutzers und der Karte her, da andernfalls der öffentliche Schlüssel E_A nicht authentisch wäre (S 41 Abschn "Authentizität der öffentlichen Schlüssel" unter Abschn 3.3.3 iVm S 64 Abschn 4.1.2.2 Abs 2 le Satz). Dieses Zertifikat Z wird von einer Zentrale aus den datenträgerindividuellen Daten ID und der individuellen Verifikationsfunktion, dem öffentlichen Schlüssel E_{ID}, mittels eines asymmetrischen Signierschemas gebildet und im intelligenten Datenträger gespeichert (erstes kennzeichnendes Merkmal).

Das Terminal verifiziert das zu ihm übertragene Zertifikat anhand des Verifikationsalgorithmus v und speichert die Daten und trägerindividuellen Daten ID und die individuelle Verifikationsfunktion E_{ID} sinnvollerweise nur vorübergehend (2. kennzeichnendes Merkmal), nämlich bis die entschlüsselte elektronische Unterschrift überprüft (letztes kennzeichnendes Merkmal) und damit die Integrität und Authentizität der Buchungsdaten erwiesen ist (S 41 Abschn "Authentizität der öffentlichen Schlüssel" iVm S 71 Bild 4.8).

Dr. Anders Obermayer Martens Dr. Zehendner

Fa