BUNDESPATENTGERICHT

20 W (pat) 8/09

_____

(Aktenzeichen)

Verkündet am
22. Juli 2013
…

B E S C H L U S S

In der Beschwerdesache

betreffend die Patentanmeldung 10 2007 045 776.8-31

…

hat der 20. Senat (Technischer Beschwerdesenat) auf die mündliche Verhandlung vom 22. Juli 2013 durch den Richter Dipl.-Ing. Kleinschmidt als Vorsitzenden, die Richterin Kopacek sowie die Richter Dipl.-Ing. Gottstein und Dipl.-Geophys. Dr. Wollny

beschlossen:

Die Beschwerde wird zurückgewiesen.

G r ü n d e

I.

Das Deutsche Patent- und Markenamt - Prüfungsstelle für Klasse H 04 L - hat die am 25. September 2007 beim Deutschen Patent- und Markenamt eingegangene Patentanmeldung mit der Bezeichnung

„Verfahren zum Schutz mindestens von Teilen von auf mindestens einem Server und/oder in mindestens einer Datenbank abgelegten, einem durch ein RFID-Tag identifizierten Produkt zugeordnete Produktdaten vor unberechtigtem Zugriff“

durch Beschluss vom 1. Dezember 2008 zurückgewiesen.

Der Zurückweisung lagen die Ansprüche 1 bis 20 vom Anmeldetag, dem 25. September 2007, zugrunde.

Zur Begründung führte die Prüfungsstelle im Wesentlichen aus, dass der Gegenstand des Anspruchs 1 nicht neu sei und verwies hierzu als relevanten Stand der Technik auf die Druckschrift

D1 EP 1 571 591 A1.

Insgesamt waren seitens der Prüfungsstelle im Prüfungsverfahren zwei Druckschriften eingeführt worden, und zwar die europäischen Offenlegungsschriften

D1 EP 1 571 591 A1
D2 EP 1 577 824 A1.

Gegen den Beschluss vom 1. Dezember 2008, der am 17. Dezember 2008 im Abholfach der Anmelderin niedergelegt wurde, hat diese mit Schreiben vom 16. Januar 2009, eingegangen beim Deutschen Patent- und Markenamt am selben Tage, Beschwerde eingelegt. Mit der nachgereichten Beschwerdebegründung vom 21. Januar 2009, eingegangen beim Deutschen Patent- und Markenamt am selben Tage, verfolgt die Anmelderin ihre Anmeldung weiter.

Die Bevollmächtigten der Anmelderin beantragen,

> den Beschluss der Prüfungsstelle für Klasse H 04 L des Deutschen Patent- und Markenamts vom 1. Dezember 2008 aufzuheben und das nachgesuchte Patent auf der Grundlage folgender Unterlagen zu erteilen:
>
> **Patentansprüche:**
>
> Patentanspruch 1, überreicht in der mündlichen Verhandlung am 22. Juli 2013, Fassung 11.25 Uhr,
> Patentansprüche 2 bis 20 vom Anmeldetag (25. September 2007)
>
> **Beschreibung:**
>
> Beschreibungsseiten 1 und 2 gemäß Schriftsatz vom 6. August 2008,
> Beschreibungsseite 3, 3 a überreicht in der mündlichen Verhandlung am 22. Juli 2013,
> Beschreibungsseiten 4 bis 15 vom Anmeldetag (25. September 2007)

Zeichnungen:

Figuren 1 bis 3 vom 16. November 2007.

Der Patentanspruch 1 lautet:

„Verfahren zum Schutz mindestens von Teilen von auf mindestens einem Server (04, 09) und/oder in mindestens einer Datenbank abgelegten, einem durch ein RFID-Tag (02, 12) identifizierten Produkt zugeordnete Produktdaten vor unberechtigtem Zugriff, bei welchem Verfahren eine Authentisierung und Berechtigungsprüfung eines Zugreifenden bei einem Server- und/oder Datenbankzugriff erfolgt,

dadurch gekennzeichnet,

dass bei einem Server- und/oder Datenbankzugriff zusätzlich ein Nachweis verlangt wird, dass sich das Produkt innerhalb des Verfügungsbereichs des Zugreifenden befindet, welcher Nachweis von dem RFID-Tag (02, 12) bei dessen Erfassung durch einen RFID-Leser (03, 06) durch ein Access-Token in Form einer Datenstruktur bereitgestellt wird, durch die das RFID-Tag (02, 12) den Zugreifenden ermächtigt, zumindest Teile der Produktdaten abzufragen und/oder zu ändern,

wobei das Access-Token einen RFID-Identifier, einen Zähler und eine Prüfsumme enthält, wobei die Prüfsumme mit einem dem Server und/oder der Datenbank und dem RFID-Tag bekannten Schlüssel, dem RFID-Identifier und dem Zähler berechnet wird,

und der Server und/oder die Datenbank mit Hilfe seines dem RFID-Identifier zugeordneten Schlüssels die Korrektheit des Access-Tokens überprüft.“

Hieran schließen sich weitere Unteransprüche 2 bis 20 an, zu deren Wortlaut auf die Ursprungsunterlagen verwiesen wird.

Die Beschwerdeführerin hält den Gegenstand der verteidigten Anspruchsfassung für patentfähig, da er durch den im Verfahren befindlichen Stand der Technik weder neuheitsschädlich vorweggenommen, noch dem Fachmann nahegelegt sei.

Bezüglich der weiteren Einzelheiten wird auf den Inhalt der Akten verwiesen.

II.

Die zulässige Beschwerde hat keinen Erfolg, da der Gegenstand des geltenden Patentanspruchs 1 mangels des Zugrundeliegens einer erfinderischen Tätigkeit nicht patentfähig ist (§ 1 Abs. 1 i. V. m. § 4 PatG):

1. Die Erfindung bezieht sich gemäß den Anmeldungsunterlagen, Seite 1, Absatz 1, auf ein Verfahren zum Schutz von auf mindestens einem Server und/oder in mindestens einer Datenbank abgelegten, einem durch ein RFID-Tag identifizierten Produkt zugeordneten Produktdaten vor unberechtigtem Zugriff. Mit anderen Worten sollen durch das erfindungsgemäße Verfahren (zumindest die Teile von) Produktdaten eines mit einem RFID-Tag gekennzeichneten Produktes, die auf einem Server und/oder in einer Datenbank abgelegt sind, vor unberechtigtem Zugriff geschützt werden.

Um Warenströme effizienter handhaben zu können, würden Produkte durch ein individuelles Radio-Frequency-Identification (RFID)-Tag gekennzeichnet. Die Produktdaten selbst seien jedoch oft auf einem Server abgespeichert. Eine auf dem RFID-Tag abgelegte Information diene nur zur Identifizierung eines Produkts, wogegen weitere, das Produkt beschreibende Daten etwa auf einem zentralen Server abgelegt seien (Seite 1, Absatz 2). In komplexen Geschäftsbeziehungen durchlaufe ein Produkt unterschiedliche Firmen mit unterschiedlichen Sicherheits-

domänen, die jeweils auf die einem Produkt zugeordneten, auf einem Server abgelegten Daten lesend und/oder schreibend zugreifen müssten. Um auf einem Server abgelegte, einem durch ein RFID-Tag identifizierten Produkt zugeordnete Daten vor einem unberechtigten Zugriff zu schützen, seien Sicherheitslösungen für die Schnittstelle zwischen RFID-Leser und RFID-Tag bekannt. Dadurch werde gewährleistet, dass nur ein berechtigter RFID-Leser Daten von einem RFID-Tag lesen bzw. schreiben könne, bzw. dass die gelesenen Daten von einem nicht manipulierten, authentisierten RFID-Tag stammten. Solche Sicherheitslösungen führten lediglich ein Prüfen der Berechtigung, Daten vom RFID-Tag selbst zu lesen bzw. zu ändern, durch (Seite 1, Absatz 3 und 4). Weiterhin sei bekannt, dass bei Abfrage von Produktdaten eines Produkts, dem ein RFID-Tag zugeordnet sei, bei einem Server eine Authentisierung und Berechtigungsprüfung stattfinde. Dabei werde durch den Server überprüft, ob die Abfrage von einem berechtigten Teilnehmer gestellt werde. Eine Überprüfung könne beispielsweise die vorgegebene Logistik-Kette berücksichtigen, d. h. wenn das mit einem RFID-Tag versehene Produkt bei einem bestimmten Teilnehmer sein sollte, dann dürfe auch nur dieser auf die Daten des Servers mit den gespeicherten Produktdaten zugreifen. Dabei handele es sich aber nur um statische Sicherheitsmechanismen, die nicht berücksichtigten, ob der auf die Datenbank bzw. den Server zugreifende Teilnehmer auch tatsächlich Zugriff auf das Produkt bzw. das zugehörige RFID-Tag habe (Seite 1, Absatz 5 bis Seite 6, Absatz 1).

Es sei daher Aufgabe der Erfindung, einen besseren Schutz vor unberechtigtem Zugriff auf einem durch ein RFID-Tag identifizierten Produkt zugeordnete, auf einem Server abgelegte Daten zu erreichen. Insbesondere solle ein unberechtigter Zugriff auf geschäftskritische Daten eines Wettbewerbers verhindert werden, beispielsweise um Wirtschaftsspionage zu erschweren (Seite 2, Absatz 2).

2. Der für die Beurteilung der Patentfähigkeit des Gegenstandes des Patentanspruchs 1 zuständige Fachmann ist ein Ingenieur der Prozesstechnik mit Fachhochschulabschluss, der über langjährige Erfahrung auf dem Gebiet der Erfassung, Nutzung und Verwaltung von Produktinformationen verfügt, wie sie etwa im Logistikbereich an der Tagesordnung sind.

3. Der antragsgemäße Verfahrensanspruch 1 lässt sich wie folgt gliedern:

M1 Verfahren zum Schutz mindestens von Teilen von auf mindestens einem Server (04, 09) und/oder in mindestens einer Datenbank abgelegten, einem durch ein RFID-Tag (02, 12) identifizierten Produkt zugeordnete Produktdaten vor unberechtigtem Zugriff,

M2 bei welchem Verfahren eine Authentisierung und Berechtigungsprüfung eines Zugreifenden bei einem Server- und/oder Datenbankzugriff erfolgt,

dadurch gekennzeichnet, dass

M3 bei einem Server- und/oder Datenbankzugriff zusätzlich ein Nachweis verlangt wird, dass sich das Produkt innerhalb des Verfügungsbereichs des Zugreifenden befindet,

M4 welcher Nachweis von dem RFID-Tag (02, 12) bei dessen Erfassung durch einen RFID-Leser (03, 06) durch ein Access-Token in Form einer Datenstruktur bereitgestellt wird,

M5 durch die das RFID-Tag (02, 12) den Zugreifenden ermächtigt, zumindest Teile der Produktdaten abzufragen und/oder zu ändern.

M6 wobei das Access-Token einen RFID-Identifier, einen Zähler und eine Prüfsumme enthält, wobei die Prüfsumme mit einem dem Server und/oder der Datenbank und dem RFID-Tag bekannten Schlüssel, dem RFID-Identifier und dem Zähler berechnet wird,

M7 und der Server und/oder die Datenbank mit Hilfe seines einem dem RFID-Identifier zugeordneten Schlüssels die Korrektheit des Access-Tokens überprüft.

Das Verfahren gemäß Patentanspruch 1 ist nicht patentfähig, da sich sein Gegenstand für den Fachmann in nahe liegender Weise aus dem Stand der Technik und seinem Fachwissen ergibt und somit nicht auf einer erfinderischen Tätigkeit beruht (§ 4 PatG).

Aus der Druckschrift EP 1 571 591 A1 (**D1**) ist ein mehrere Schritte aufweisendes Verfahren zum Schutz mindestens von Teilen von auf mindestens einem Server und/oder in mindestens einer Datenbank abgelegten, einem durch ein RFID-Tag (10) identifizierten Produkt (1) zugeordneten Produktdaten vor unberechtigtem Zugriff, bekannt (Absatz [0019]: „… wird der Zugriff zur gewünschten Information erst dann gewährt, wenn die vom RFID-Tag 10 erhaltene Identifizierung des Benutzers akzeptiert wurde.“; Absatz [0057]: „ … Vorteil, dass der Zugriff auf die gewünschte Information oder Dienstleistung nur dem Benutzer gewährleistet wird, der den passenden RFID-Tag und die SIM-Karte vorweisen kann.“; Merkmal **M1**).

In diesem Verfahren erfolgt auch eine Authentisierung und Berechtigungsprüfung eines Zugreifenden bei einem Server- und/oder Datenbankzugriff (Absatz [0041]: „Der Server 5 kann auch die Identität oder das aus dieser Identität ermittelte Alias des Benutzers des Mobilgeräts 3 mit einem Authentifikationsteil 52 prüfen. … In diesem Fall kann die Identität des Benutzers beispielsweise anhand der IMSI (International Mobile Subscriber Identity) oder einer anderen Mobilteilnehmer-Identität in der SIM-Karte zuverlässig ermittelt werden.“ i. V. m. Absatz [0057]: „Das erfindungsgemäße Verfahren hat somit den Vorteil, dass der Zugriff auf die gewünschte Information oder Dienstleistung nur dem Benutzer gewährleistet wird, der den passenden RFID-Tag und die SIM-Karte vorweisen kann.“; Anspruch 1 i. V. m. Anspruch 4, insbesondere „Das Verfahren …, in welchem das … Sicherheitselement zur Identifizierung des Benutzers gegenüber dem benannten RFID-

Tag (20) und/oder gegenüber dem Server (5, 7) [dient], …, wobei Zugriff … erst dann gewährt wird, wenn der Benutzer vom benannten RFID-Tag (10) und/oder vom benannten Server (5, 7) authentifiziert und autorisiert wurde.“; Merkmal **M2**).

Es ist auch bekannt, dass bei einem Server- und/oder Datenbankzugriff zusätzlich ein Nachweis verlangt wird, dass sich das Produkt innerhalb des Verfügungsbereichs des Zugreifenden befindet. Dies lässt sich direkt aus der funktionsnotwendigen räumlichen Nähe des Lesegerätes von wenigen Metern zum RFID-Tag ableiten, woraus nach der allgemeinen Lebenserfahrung auch eine höchstwahrscheinliche Verfügungsgewalt über das Produkt resultiert i. V. m. der Tatsache, dass auf eine Leseanfrage der in der Druckschrift **D1** als gemeinsam agierende Leseeinheiten „RFID-Leseteil 2“ und „Mobilgerät 3“ zu verstehenden Bestandteile der Nachweis durch die Antwort des RFID-Tags (10) gegeben ist (Absatz [0017]: „Der Nachweis eines Lesegeräts, dass es die erwartete Antwort [auf eine Zufallsnummer des RFID-Tags hin] generieren kann, kann als Identifizierung verwendet werden.“ i. V. m. Absatz [0020]: „…, indem das RFID-Tag zuerst ein Challenge an die SIM-Karte 30 [als Bestandteil der „Leseeinheiten 2, 3“ zu verstehen] sendet, aus welcher die cryptographischen Mittel 301 der SIM-Karte 30 eine Antwort errechnen. Die Antwort wird an das RFID-Tag gesendet, welches erst dann Zugriff auf den gewünschten Code (oder den Speicherbereich) gewährt, wenn die erhaltene Antwort richtig ist.“; Merkmal **M3**).

Der Nachweis wird auch hier vom RFID-Tag 10 bei seiner Erfassung durch einen RFID-Leser 2 bereitgestellt und zwar durch den als Access-Token in Form einer Datenstruktur zu interpretierenden „Code 100“, der im RFID-Tag abgelegt ist (Absatz [0024]: „Der … Code identifiziert eindeutig jedes bestimmte RFID-Tag 1[0], jedes RFID-Tag hat vorzugsweise einen anderen Code 100.“). Dieser ermächtigt auch den Zugreifenden, zumindest Teile der Produktdaten abzufragen und/oder zu ändern (Absatz [0019] i. V. m. Anspruch 1: „… das Produkt (1) wird mit mindestens einem Code (100) markiert, der in einem RFID-Tag (10) abgelegt wird, der benannte Code wird über eine erste kontaktlose Schnittstelle mit einem Mobilgerät

oder mit einem in einem Mobilgerät integrierten RFID-Lesegerät (2, 3) gelesen, …, das benannte Mobilgerät (2, 3) sendet den benannten Code … an einen Namen-Dienstserver (6), der benannte Namen-Dienstserver (6) antwortet mit der Adresse einer oder mehrerer Hypertext-Seiten, es wird anhand der benannten Hypertext-Seiten auf die gewünschte Information (7) zugegriffen …“ , und Anspruch 12: „[wobei]… die benannte Identifizierungskarte (30) und das benannte RFID-Tag (10) beide vorgewiesen werden, um Zugriff auf die benannte gewünschte Information zu erhalten.“; Merkmale **M4** und **M5**).

Um den Schutz von Produktdaten im RFID-Kontext weiter zu verbessern, ist der Fachmann ausgehend von der Druckschrift EP 1 571 591 A1 (**D1**) gehalten, sich weiter auf dem Gebiet digitaler Kommunikationsmittel zu informieren, wie sie bei Zugangskontrollen Verwendung finden und dort speziell bei den Sicherungsmaßnahmen für den Datenaustausch und die Kommunikation zwischen einzelnen Teilnehmern. Wie der Fachmann weiß, kommt als eine der einfachsten Sicherungsmaßnahmen für digitale Zugangs-/Zugriffsberechtigungen neben einer individuellen Identifizierungsinformation (z. B. digitale Klarzahl-Identifikationsnummer) oft eine Prüfsumme sowie weitere mit dieser verknüpfte digitale Datenblöcke oder Algorithmen zum Einsatz. Derartige Verknüpfungen können beispielsweise auch zu Verschlüsselungen führen. Den Einsatz von Prüfsummen und Verschlüsselungen lehrt den Fachmann im Kontext ohnehin bereits die Druckschrift EP 1 571 591 A1 (**D1**), wenngleich nur in Form des Antwort-Datenpakets („Antwort“) eines RFID-Tags, das auf eine Anfrage eines Lesegeräts hin von diesem abgesandt wird. In diesem werden so genannte „Prüfdaten“ im Zusammenhang mit dem den RFID-Tag individualisierenden „Code“ zusammen verschickt, wobei letzterer einer Verschlüsselung unterliegen kann (Absatz [0024] und [0025] i. V. m. Figur 2: „Die Antwort 1000 des RFID-Tags 10 auf eine Anfrage des Leseteils 2 umfasst vorzugsweise einen Vorsatz 1001, redundante Prüfdaten 1002 und erst dann einen Code 100.“ i. V. m. Absatz [0023]: „… bevor der gewünschte Code 100 (vorzugsweise verschlüsselt) über die … Schnittstelle … gesendet wird.“).

Auf diesem Kenntnisstand aufbauend, ist es dem Fachmann im gegebenen Kontext ohne Weiteres nahe gelegt, das mit der oben genannten „Antwort“ bereits vorliegende abschnittsweise Konzept auch im Rahmen des „Codes 100“, aber in erweiterter Form als Access-Token mit mehreren Abschnitten, zu verwirklichen. Bei derartigem Vorgehen stehen ihm vorteilhafter Weise im Access-Token dann mehrere Datenblöcke zur Verfügung, die im Rahmen einer zusätzlichen Verarbeitungsstufe zu einer gegenüber dem Stand der Technik sichereren Kennung für den RFID-Tag weiterverarbeitet werden können. Die konkrete Befüllung und/oder Berechnung der genannten Abschnitte hängt vom jeweiligen Einsatzbereich, den technischen Randbedingungen sowie der angestrebten Sicherheitsstufe ab und geht zur Überzeugung des Senats nicht über das fachmännischen Wissen und Können hinaus. Der Fachmann wird sicher in nahe liegender Weise einen Abschnitt/Datenblock für eine digitale Kennung des RFID-Tags („RFID-Identifier“) vorsehen (vgl. Anregung aus dem „Code 100“ der Druckschrift EP 1 571 591 A1 (**D1**)), der je nach technischem Kontext von weiteren Abschnitten gefolgt wird, wie einem Abschnitt/Datenblock, der beispielsweise die Zahl der an einem RFID-Tag vorgenommenen Lesevorgänge für einen zeitlichen Logistikkontext repräsentiert (vgl. Anregung aus der Druckschrift EP 1 571 591 A1 (**D1**), Absatz [0036]: „Zeitstempel“). Um diese beiden - und ggfls. weitere - Abschnitte zur Sicherung der Datenblöcke zu verknüpfen, kann er letztlich auch eine Prüfsumme vorsehen, die als abschließender Datenblock in einem letzten Abschnitt des Access-Tokens abgelegt wird.

Dass bei einem derartigen Vorgehen die Berechnung der genannten Prüfsumme im Access-Token seitens all der Teilnehmer (Server/Datenbank), auf die mittels des Access-Tokens Zugriff erlangt werden soll, erfolgen können muss, ist eine kausale Notwendigkeit, damit die angestrebte Funktionalität des auf einen Prüfsummenvergleich aufbauenden digitalen Sicherungsvorgangs überhaupt eine bestimmungsgemäße Wirkung entfalten kann (vgl. Anregung aus der Druckschrift EP 1 571 591 A1 (**D1**), Absatz [0041]: „Der Server 5 kann … die Identität oder das aus dieser … ermittelte Alias des Benutzers des Mobilgeräts 3 mit einem Authenti-

fikationsteil 52 prüfen. … End-zu-End Benutzeridentifizierung und/oder Authentifizierung an Hand eines Schlüsselpaars und eines asymmetrischen Signierungsverfahrens kann im Rahmen der Erfindung auch eingesetzt werden, …“).

Um die Zugriffssicherheit im gesamten Teilnehmersystem zu erhöhen, ist es darüber hinaus im Verfahrensablauf nahe liegend, eine Prüfsummenberechnung unter Einbeziehung des digitalen Inhalts möglichst vieler auf dem Access-Token vorhandener, dafür geeigneter Datenblöcke vorzunehmen. Vor dem Hintergrund der Druckschrift EP 1 571 591 A1 (**D1**) ist zudem bereits bekannt, hierfür nicht nur eine bloße digitale Addition vorzunehmen, sondern eine Prüfsummenberechnung mittels bestimmten Teilnehmern (RFID-Tag, Mobilgerät) zur Verfügung stehender Schlüssel durchzuführen (Figur 1 i. V. m. Absatz [0014] und Absatz [0036]: „cryptographisches Sicherheitselement 301“; Absatz [0016]: „cryptographische Mittel 102“; Absatz [0019]: „Mit den cryptographischen Sicherheitselementen in der SIM-Karte 30 und/oder im RFID-Tag 10, kann die Datenübertragung zwischen dem RFID-Tag 10 und dem RFID-Lesegerät 2 verschlüsselt werden.“). Damit für die Erteilung einer Zugriffsberechtigung die bisherigen Verfahrensschritte nicht überflüssigerweise durchgeführt wurden, ist es daher eine sicherheitstechnische Funktionsnotwendigkeit, dass ein o. g. Teilnehmer (Server/Datenbank), auf Basis des bei ihm einem RFID-Tag bzw. dessen RFID-Identifier zugeordneten Schlüssels, auch die Zugriffsberechtigung/Korrektheit des gesamten Access-Tokens und nicht nur der o. g. Prüfsumme ermitteln können muss (Merkmale **M6** und **M7**).

Damit ergibt sich für den Fachmann der Gegenstand des Patentanspruchs 1 in naheliegender Weise aus Kenntnis der Druckschrift EP 1 571 591 A1 (**D1**) zusammen mit seinem Fachwissen. Er beruht somit nicht auf einer erfinderischen Tätigkeit und ist daher auch nicht patentfähig.

Mit dem Patentanspruch 1 sind auch die auf diesen rückbezogenen Ansprüche 2 bis 20 nicht gewährbar, da ein Patent nur so erteilt werden kann, wie es beantragt ist (BGH, Beschluss vom 26. September 1996 – X ZB 18/95, GRUR 1997, 120 - elektrisches Speicherheizgerät, mit weiteren Nachweisen).

Kleinschmidt Kopacek Gottstein Dr. Wollny

Pü