



BUNDESGERICHTSHOF

IM NAMEN DES VOLKES

URTEIL

X ZR 139/17

Verkündet am:
1. Oktober 2019
Anderer
Justizangestellte
als Urkundsbeamtin
der Geschäftsstelle

in der Patentnichtigkeitssache

Der X. Zivilsenat des Bundesgerichtshofs hat auf die mündliche Verhandlung vom 1. Oktober 2019 durch die Richter Dr. Bacher, Dr. Grabinski und Dr. Deichfuß und die Richterinnen Dr. Kober-Dehm und Dr. Rombach

für Recht erkannt:

Die Berufung gegen das Urteil des 5. Senats (Nichtigkeitssenats) des Bundespatentgerichts vom 11. September 2017 wird auf Kosten der Klägerin zurückgewiesen.

Von Rechts wegen

Tatbestand:

- 1 Der Beklagte war bis zum 16. April 2016 Inhaber des mit Wirkung für die Bundesrepublik Deutschland erteilten europäischen Patents 1 259 046 (Streitpatents), das am 22. April 2002 unter Inanspruchnahme der Priorität einer österreichischen Patentanmeldung vom 23. April 2001 angemeldet worden ist. Das Europäische Patentamt wies einen Einspruch gegen das Streitpatent zurück. Die Beschwerde gegen diese Entscheidung blieb erfolglos.
- 2 Patentanspruch 1, auf den fünf weitere Ansprüche rückbezogen sind, lautet:

"Anlage für die sichere Durchführung von Transaktionen zwischen informationsverarbeitenden Systemen mit einem Terminal (102), das zur Eingabe einer Benutzerkennung dient, mit einer Auswerteeinheit (106), die mit dem Terminal (102) über ein primäres Netz (101) verbunden ist und im Wesentlichen aus einer Speicher- und Prozesseinheit besteht, welche zur Speicherung von Benutzerstammdaten und laufenden Transaktionsdaten dient, mit einem Codegenerator, der einen Sicherheitscode erzeugt, mit einer Sendeeinrichtung, die den Sicherheitscode über ein sekundäres Netz (107) an ein Empfangsgerät (108) sendet, und mit einer Eingabemöglichkeit für den Sicherheitscode am Terminal und einer Überprüfung des eingegebenen Sicherheitscodes auf Gültigkeit durch die Auswerteeinheit (106), dadurch gekennzeichnet, dass die Auswerteeinheit (106) einen zusätzlichen Codegenerator zur Erstellung eines Zusatzcodes aufweist und eine zusätzliche Sendeeinrichtung zur Übermittlung des Zusatzcodes über das primäre Netz (101) an das Terminal (102) und zur Ausgabe des Zusatzcodes aufweist, wobei das Terminal neben der Eingabemöglichkeit des Sicherheitscodes eine Ausgabe- und Eingabemöglichkeit für den Zusatzcode aufweist und die Auswerteeinheit (106) derart ausgestaltet ist, dass diese den eingegebenen Zusatzcode überprüft und bei Gültigkeit von eingegebenem Sicherheitscode und Zusatzcode die Transaktion autorisiert."
- 3 Die Klägerin hat geltend gemacht, der Gegenstand des Streitpatents sei nicht patentfähig. Der Beklagte hat das Streitpatent in der erteilten Fassung und hilfsweise in einer geänderten Fassung verteidigt.
- 4 Das Patentgericht hat die Klage abgewiesen. Hiergegen richtet sich die Berufung der Klägerin, die ihren erstinstanzlichen Antrag weiterverfolgt. Der Beklagte tritt dem Rechtsmittel entgegen.

Entscheidungsgründe:

5 Die zulässige Berufung bleibt erfolglos.

6 I. Das Streitpatent betrifft eine Anlage zur sicheren Durchführung von
Transaktionen zwischen informationsverarbeitenden Systemen.

7 1. Als Beispiele für Bereiche, in denen solche Transaktionen erfolgen, wer-
den in der Streitpatentschrift das Online-Banking und der Online-Handel genannt. Im
Stand der Technik war es nach Angabe der Streitpatentschrift bekannt, für die siche-
re Durchführung von Transaktionen Benutzerkennungen, Passwörter, PINs (Persön-
liche Identifikationsnummern) oder TANs (Transaktionsnummern) zu verwenden, um
den Nutzer zu identifizieren und Transaktionen zu autorisieren. Während Benutzer-
kennungen und PINs bei nachlässiger Handhabung durch den Nutzer ein erhebli-
ches Risiko begründeten, habe sich die Nutzung von TANs, die über einen sekundä-
ren Leitungsweg übermittelt werden, als relativ sicher erwiesen. Allerdings bestünden
auch hier latente Sicherheitsprobleme, etwa wenn eine dem Nutzer zugesendete
TAN-Liste von diesem nicht sicher aufbewahrt werde. Auch bei elektronischer Über-
mittlung einer TAN bestünden gewisse Risiken, etwa bei der Fälschung von Anmel-
debildschirmen oder in den Fällen, in denen Dritte Zugriff auf das Gerät haben könn-
ten, an das die TAN übermittelt werde. Es bestehe die Gefahr, dass eine unbefugte
Person den kompletten Autorisierungscode erhalte und dadurch in die Lage versetzt
werde, eine Transaktion zu autorisieren.

8 2. Dem Streitpatent liegt vor diesem Hintergrund das technische Problem
zugrunde, eine Anlage mit erhöhter Transaktionssicherheit bereitzustellen.

9 3. Diese Aufgabe soll erfindungsgemäß durch eine Vorrichtung gelöst wer-
den, deren Merkmale sich wie folgt gliedern lassen (Merkmalsgliederung des Patent-
gerichts in eckigen Klammern):

1. Anlage für die sichere Durchführung von Transaktionen zwischen informationsverarbeitenden Systemen mit einem Terminal und einer Auswerteeinheit. [M1, M2 teilweise, M3]
2. Die Auswerteeinheit
 - a) ist mit dem Terminal über ein primäres Netz verbunden, [M3.1]
 - b) besteht im Wesentlichen aus einer Speicher- und Prozessoreinheit, die zur Speicherung von Benutzerstammdaten und laufenden Transaktionsdaten dient, [M3.2]
 - c) umfasst einen Codegenerator, der einen Sicherheitscode erzeugt, und eine Sendeeinrichtung, die diesen über ein sekundäres Netz an ein Empfangsgerät sendet, [M4 und M5]
 - d) umfasst einen zusätzlichen Codegenerator zur Erstellung eines Zusatzcodes und eine zusätzliche Sendeeinrichtung zur dessen Übermittlung über das primäre Netz an das Terminal. [M8, M8.1, M8.2]
3. Das Terminal
 - a) dient der Eingabe einer Benutzerkennung, [M2 Rest]
 - b) ermöglicht die Eingabe des Sicherheitscodes, [M6]
 - c) ermöglicht die Ausgabe und die Eingabe des Zusatzcodes. [M9]
4. Die Auswerteeinheit überprüft den eingegebenen Sicherheitscode und den eingegebenen Zusatzcode und autorisiert bei deren Gültigkeit die Transaktion. [M7, M10]

10 Der Autorisierungscode ist danach aufgeteilt in einen Sicherheitscode und einen Zusatzcode, die auf unterschiedlichen Wegen übermittelt werden. Beide müssen eingegeben und von der Auswerteeinheit als gültig erkannt werden, damit die Transaktion autorisiert wird.

11 4. Im Hinblick auf einige Merkmale bedarf der Patentanspruch der Erläuterung:

12 a) Der Begriff der Transaktion ist in der Streitpatentschrift nicht definiert. Als Beispiele für die Anwendung der Lehre sind dort das Online-Banking, ein Bezahlvorgang im Online-Handel oder die Gewährung des Zutritts zu einem Gebäude genannt. In Absatz 2 der Beschreibung sind mit PIN und TAN einige Instrumente benannt, wie sie zur Sicherung etwa von Banküberweisungen, Wertpapierkäufen und -verkäufen und dergleichen eingesetzt werden. Diesen Vorgängen ist gemeinsam, dass sie aus Sicherheitsgründen einer besonderen Autorisierung oder Authentifizierung bedürfen. Charakteristisch für eine Transaktion im Sinne des Streitpatents ist danach, dass es sich um einzelne Vorgänge innerhalb einer Kommunikation zwischen zwei informationsverarbeitenden Systemen handelt, für die eine besondere, erhöhte Sicherheit gewünscht wird. Dieses Bedürfnis nach einer erhöhten Sicherheit kann sich insbesondere daraus ergeben, dass vermögensrelevante Änderungen vorgenommen oder sensible Daten angezeigt werden sollen.

13 Die Bedeutung des Begriffs in Patentanspruch 1 ist damit enger als der im Bereich der Datenbanktechnik gebräuchliche Begriff der Transaktion als einer Folge von Programmschritten, die den Datenbestand nach fehlerfreier, vollständiger Ausführung in einem konsistenten Zustand hinterlassen. Zwar wird eine Transaktion im Sinne des Streitpatents regelmäßig auch eine Veränderung des Datenbestands bewirken. Nicht jede Veränderung des Datenbestands ist aber zwangsläufig eine Transaktion im Sinne des Streitpatents. Erst recht ist mit diesem Begriff nicht jeder Kommunikationsvorgang im World Wide Web, etwa jeder Austausch von Daten nach dem Client-Server-Modell gemeint.

14 b) Das Patentgericht hat zutreffend angenommen, dass es sich bei einem Zusatzcode im Sinne des Streitpatents um einen transaktionsspezifischen Code handelt.

15 Wie sich aus Merkmal 4 ergibt, dienen der Sicherheitscode und der Zusatzcode der Autorisierung der Transaktion, sollen also gewährleisten, dass nur eine berechnete Person diese auslösen kann. Sicherheitscode wie Zusatzcode müssen daher in einer Beziehung zur Transaktion im oben erläuterten Sinne stehen. Sicherheits- und Zusatzcode sind nach der geschützten Lehre die Instrumente, mit denen dem erhöhten Sicherheitsbedürfnis Rechnung getragen wird. Damit handelt es sich beim Zusatzcode - nicht anders als beim Sicherheitscode - um einen Code, der gerade für diese besondere Situation vorgesehen ist. Dies schließt nicht schlechterdings aus, den Code zugleich für andere Zwecke zu nutzen. Es darf sich aber nicht um ein Mittel handeln, mit dem die Kommunikation zwischen den beteiligten informationsverarbeitenden Systemen in ihrer Gesamtheit geschützt oder verwaltet wird. Der Zusatzcode muss vielmehr in einzelnen dafür vorgesehenen Situationen als weiteres Sicherungsmittel zu den Mitteln für die grundlegende Absicherung der Kommunikationsbeziehung hinzutreten.

16 II. Das Patentgericht hat seine Entscheidung im Wesentlichen wie folgt begründet:

17 Der Gegenstand von Patentanspruch 1 werde dem Fachmann, der von der deutschen Offenlegungsschrift 197 18 103 (NK12) oder von der europäischen Patentanmeldung 1 065 634 (NK14) ausgehe, weder durch das Buch von Scott Mitchell und James Atkinson (SAMS Teach Yourself Active Server Pages 3.0 in 21 Days, NK13), noch durch die Aufsätze von Henrik Loser (Techniken für Web-basierte Datenbankanwendungen, Informatik Forsch. Entw. 1998, S. 196 ff., NK 15) und Arun Iyengar (Dynamic Argument Embedding: Preserving State on the World Wide Web, IEEE Internet Computing 1997, S. 50 ff., NK16) nahegelegt. In diesen Dokumenten gehe es jeweils nur um die netzwerkseitige Verwaltung von Verbindungen zwischen Server und Client. Die dafür erörterten Instrumente wie Session-IDs, Cookies und Statusparameter mit User-ID betreffen jedoch jeweils die Sitzung (*session*) und seien nicht transaktionsspezifisch. Aus ihnen ergebe sich daher keine Anregung, einen Zusatzcode vorzusehen, der transaktionsspezifisch sei und der Autorisierung einer

Transaktion diene. Zudem vermittele keine dieser Schriften eine technische Lehre, wonach zwei Codegeneratoren und zwei Sendeeinrichtungen dem Erzeugen und Senden eines Sicherheits- und eines Zusatzcodes dienen.

18 Eine solche Anregung ergebe sich auch nicht aus dem US-Patent 6 061 741 (NK18). Der Fachmann, der von NK12 oder NK14 ausgehe, habe bereits keinen Anlass, die NK18 heranzuziehen, denn dieses Dokument befasse sich nicht mit der Autorisierung von Transaktionen, sondern mit der Synchronisation von verbindungslosen Anwendungen in Client-Server-Systemen.

19 III. Diese Beurteilung hält der Überprüfung im Berufungsrechtszug stand.

20 1. Das Patentgericht hat mit zutreffenden Erwägungen, die von der Berufung nicht angegriffen werden, dargelegt, warum der Fachmann, der von NK12 oder NK14 ausgeht, durch NK13, NK15 oder NK16 keine Anregung erhält, einen Zusatzcode vorzusehen, der der Autorisierung einer Transaktion dient und über das primäre Netz an das Terminal übertragen wird.

21 2. Entgegen der Auffassung der Klägerin wurde dem Fachmann, der von NK12 oder NK14 ausgeht, auch durch NK18 keine solche Anregung vermittelt.

22 a) Zutreffend hat das Patentgericht angenommen, dass NK12 oder NK14, die unter den hier interessierenden Aspekten weitgehend übereinstimmen, den Ausgangspunkt der Bemühungen des Fachmanns darstellten.

23 NK12 schlägt für die Autorisierung von Transaktionen in Datenübertragungssystemen, etwa für das Online-Banking, vor, dass dem Benutzer, zu dem mittels informationsverarbeitender Systeme, etwa über das Internet, unter Nutzung eines Passworts oder dergleichen eine Verbindung aufgebaut wurde, über einen anderen Übertragungsweg eine TAN übermittelt wird, die der Benutzer eingibt, die sodann überprüft wird und bei deren Gültigkeit die Autorisierung der Transaktion erfolgt. Als Beispiele sind dort die Übersendung einer TAN an ein Mobiltelefon, an einen Pager oder ein Faxgerät aufgeführt. Die dort beschriebene Vorgehensweise nimmt die

Merkmale 1, 2a bis 2c und 3a und 3b von Anspruch 1 des Streitpatents vorweg. Die TAN entspricht dem Sicherheitscode im Sinne von Merkmal 2c und 3b.

24 Nicht offenbart ist dagegen die Erzeugung und Übermittlung eines Zusatzcodes über das primäre Netz, die Ausgabe und Eingabe dieses Zusatzcodes und dessen Prüfung zur Autorisierung der Transaktion.

25 b) NK18 vermittelte dem Fachmann nicht die Anregung, zur Erhöhung der Sicherheit bei der Durchführung von Transaktionen zusätzlich zu einem Sicherheitscode, der über ein sekundäres Netz übermittelt wird, einen Zusatzcode über das primäre Netz zu übermitteln und beide Codes für die Autorisierung der Transaktion einzusetzen.

26 aa) NK18 erläutert, dass es in Systemen wie dem Internet, in dem die Verbindung zwischen Client und Server nicht dauerhaft besteht, sondern immer wieder unterbrochen und wiederhergestellt wird, vielfach einen Mechanismus zur Synchronisierung der Verbindung bedarf. Dieser solle gewährleisten, dass Server und Client wechselseitig prüfen und erkennen können, auf welchem Stand sich der jeweils andere Teil befindet. Auf diese Weise solle etwa sichergestellt werden, dass die Reaktion eines Verbindungspartners auf eine bestimmte Anfrage richtig zugeordnet werden kann, obwohl die Kommunikation zwischen Client und Server immer wieder unterbrochen wird.

27 In NK18 ist zwar verschiedentlich auch von Transaktionen (*transactions*) die Rede. Dieser Begriff bezeichnet dort jedoch, wie sich aus dem Zusammenhang der NK18 ergibt, nicht einzelne Vorgänge mit erhöhtem Sicherheitsbedürfnis, sondern grundsätzlich jeden Schritt eines Kommunikationszyklus oder einer Sitzung (s. insbesondere Sp. 2 Z. 46 f., Sp. 3 Z. 33 ff.).

28 NK18 schlägt vor, zur Synchronisierung der Verbindung Sitzungstoken zu verwenden, die einen Client-Token und einen Panel-Token umfassen. Bei einem Client-Token handelt es sich um einen Code, der dazu dient, den Client zu identifizie-

ren, bei einem Panel-Token um einen Code, der Informationen über den aktuellen Zustand dieses Clients vermittelt. Ein solcher Token kann nach NK18 etwa durch die Bildung einer Prüfsumme erstellt werden, die den zuletzt angezeigten Bildschirminhalt repräsentiert.

29 bb) NK18 spricht darüber hinaus die Möglichkeit an, solche Token zu nutzen, um bestimmte Objekte mit einer „Flagge“ unverwechselbar zu kennzeichnen und weiter vorzusehen, dass ein Anwender über eine bestimmte, „passende“ Signatur verfügen müsse, um in Bezug auf dieses Objekt als berechtigt angesehen zu werden (Sp. 2, Z. 49 ff.).

30 Damit ist zwar aufgezeigt, dass solche Token nicht nur zur Synchronisation genutzt werden können, sondern auch für andere Zwecke, etwa zur Prüfung von Berechtigungen. Entgegen der Auffassung der Klägerin ergab sich daraus jedoch nicht die Anregung, die in NK18 offenbarten Token als zusätzliches Sicherungsmittel für Kommunikationsvorgänge der in NK12 und NK14 offenbarten Art einzusetzen.

31 Zwar war es im Stand der Technik bekannt, unterschiedliche Maßnahmen zur Berechtigungsprüfung vorzusehen und für einzelne, besonders sicherungsbedürftige Vorgänge mehrere solcher Instrumente nebeneinander zum Einsatz zu bringen. Daraus ergab sich aber nicht die Anregung, die in NK18 in erster Linie für Synchronisierungszwecke und damit zur Absicherung der Kommunikationsbeziehung insgesamt eingesetzten Token als zusätzliches Sicherungsmittel für besonders sicherungsbedürftige Vorgänge einzusetzen. Der in NK18 enthaltene Hinweis, dass solche Token auch zur Authentifizierung eines Benutzers eingesetzt werden können, mag dem Fachmann Anlass gegeben haben, sie anstelle eines Passworts, einer PIN oder möglicherweise einer TAN in Betracht zu ziehen. Eine Anregung, die in NK12 und NK14 offenbarten Vorgehensweisen, bei denen die TAN aus Sicherheitsgründen auf einem separaten Weg übertragen wird, dahin zu ergänzen, dass zusätzlich auf dem primären Übermittlungsweg ein Token übersendet und zusammen mit der TAN zur Autorisierung eines besonders sicherungsbedürftigen Vorgangs herangezogen wird, ergab sich indes auch daraus nicht.

32 IV. Die Kostenentscheidung beruht auf § 121 Abs. 2 PatG sowie § 97 Abs. 1 ZPO.

Bacher

Grabinski

Deichfuß

Kober-Dehm

Rombach

Vorinstanz:

Bundespatentgericht, Entscheidung vom 11.09.2017 - 5 Ni 52/15 (EP) -