BUNDESGERICHTSHOF

IM NAMEN DES VOLKES

URTEIL

X ZR 41/19

Verkündet am:
30. März 2021
Zöller
Justizangestellte
als Urkundsbeamtin
der Geschäftsstelle

in der Patentnichtigkeitssache

ECLI:DE:BGH:2021:300321UXZR41.19.0

Der X. Zivilsenat des Bundesgerichtshofs hat auf die mündliche Verhandlung vom 30. März 2021 durch den Vorsitzenden Richter Dr. Bacher, die Richter Dr. Grabinski und Hoffmann, die Richterin Dr. Kober-Dehm sowie den Richter Dr. Rensen

für Recht erkannt:

Die Berufung gegen das Urteil des 2. Senats (Nichtigkeitssenats) des Bundespatentgerichts vom 24. Januar 2019 wird auf Kosten der Beklagten zurückgewiesen.

Von Rechts wegen

Tatbestand:

1 Die Beklagte ist Inhaberin des mit Wirkung für die Bundesrepublik Deutschland erteilten europäischen Patents 1 304 002 (Streitpatents), das am 28. Juni 2001 unter Inanspruchnahme einer finnischen Priorität vom 30. Juni 2000 angemeldet wurde und die Datenverschlüsselung zwischen einem Endgerät und einem drahtlosen Telekommunikationssystem wie insbesondere WLAN (Wireless Local Area Networks) betrifft.

2 Patentanspruch 11, gegen den sich die Nichtigkeitsklagen zuletzt schon in erster Instanz allein gerichtet haben, lautet in der Verfahrenssprache:

> A wireless terminal comprising a transceiver for establishing a wireless connection with an access point in a wireless local area network and an identity module for calculating (213) at least one first ciphering key according to a public land mobile network using a secret key stored in the identity module and at least one challenge code sent by the mobile network, characterized in that
> the terminal comprises second calculation means for calculating (217) a second ciphering key using said at least one first ciphering key, and
> the terminal comprises ciphering means for enciphering/deciphering (311) the data transmitted between the terminal and the access point using said second ciphering key.

3 Die Klägerinnen haben geltend gemacht, dem Gegenstand dieses Anspruchs fehle die Patentfähigkeit. Die Klägerinnen zu 2 und 3 haben sich zudem darauf berufen, dass die Erfindung nicht ausführbar offenbart sei. Die Beklagte hat das Streitpatent in der erteilten Fassung sowie hilfsweise in vierzehn geänderten Fassungen verteidigt.

4 Das Patentgericht hat das Streitpatent im beantragten Umfang für nichtig erklärt. Mit ihrer Berufung verfolgt die Beklagte ihre erstinstanzlichen Hilfsanträge 1 bis 4 weiter. Die Klägerinnen treten dem Rechtsmittel entgegen.

Entscheidungsgründe:

5 Die zulässige Berufung der Beklagten bleibt ohne Erfolg.

6 I. Das Streitpatent betrifft die Datenverschlüsselung zwischen einem Endgerät und einem drahtlosen Telekommunikationssystem, insbesondere einem WLAN (Wireless Local Area Network).

7 1. In der Streitpatentschrift wird ausgeführt, neben Mobilfunknetzen seien verschiedene drahtlose lokale Netze gebräuchlich geworden, beispielsweise solche nach dem Standard IEEE802.11.

8 Um den Datenverkehr zwischen einem Endgerät und einem Zugangspunkt zu verschlüsseln, sehe der Standard IEEE802.11 eine Funktion namens Wired Equivalent Privacy (WEP) auf der Schicht 2 (MAC) vor. Diese basiere auf einem symmetrischen Algorithmus, bei dem derselbe Schlüssel für das Verschlüsseln und Entschlüsseln verwendet werde. Dieser Schlüssel müsse vorab im Endgerät und im Zugangspunkt gespeichert werden. Unterschiedliche Schlüssel hinzuzufügen sei schwierig. Deshalb sei es nicht immer möglich, eine sichere Datenübertragung für Endgeräte anzubieten, die sich in verschiedenen Netzen bewegten.

9 Für das GSM-System sei ein Verschlüsselungsverfahren bekannt, bei dem ein Schlüssel auf der Basis eines geheimen Parameters Ki sowie eine Zufallszahl RAND erzeugt würden, ferner eine Signalisierung zwischen einer Mobilstation und einem GSM-Netz in Bezug auf Authentifizierung und Schlüsselverwaltung.

10 2. Das Streitpatent betrifft vor diesem Hintergrund das technische Problem, eine sichere Datenverschlüsselung in drahtlosen lokalen Netzen auch für Endgeräte, die sich in vielen verschiedenen Netzen bewegen, auf möglichst einfache Weise zu ermöglichen.

11 3. Zur Lösung dieser Aufgabe schlägt Patentanspruch 11 in der Fassung des erstinstanzlichen Hilfsantrags 1 und jetzigen Hauptantrags ein Endgerät mit folgenden Merkmalen vor (Änderungen gegenüber der erteilten Fassung sind hervorgehoben):

> 11 Drahtloses Endgerät, umfassend
>
> 11.1 einen Sende-Empfänger zum Aufbauen einer drahtlosen Verbindung mit einem Zugangspunkt in einem drahtlosen, lokalen Netzwerk;
>
> 11.2 ein Identitätsmodul zum Berechnen (213) von ~~mindestens~~ mehr als einem ersten Verschlüsselungsschlüssel gemäß einem öffentlichen landgestützten Mobilnetz unter Verwendung eines Geheimschlüssels, welcher in dem Identitätsmodul gespeichert ist, und ~~mindestens~~ mehr als einem Challenge-Code, welcher von dem Mobilnetzwerk gesendet wird;
>
> 11.3 zweite Berechnungsmittel zum Berechnen (217) eines zweiten Verschlüsselungsschlüssels unter Verwendung des ~~mindestens~~ mehr als einen ersten Verschlüsselungsschlüssels;
>
> 11.4 Verschlüsselungsmittel zum Verschlüsseln/Entschlüsseln (311) der Daten, die zwischen dem Endgerät und dem Zugangspunkt übertragen werden, unter Verwendung des zweiten Verschlüsselungsschlüssels.

12 4. Einige Merkmale bedürfen näherer Betrachtung.

13 a) Ein drahtloses lokales Netzwerk im Sinne von Merkmal 1 ist ein Netzwerk, in dem Endgeräte über Funk mit einem Zugangspunkt kommunizieren können.

14 Im Vergleich zu einem Mobilfunk-Netzwerk wie etwa GSM ist der Bereich, den der Zugangspunkt abdeckt, in der Regel deutlich geringer.

15 Im Prioritätszeitpunkt gab es für drahtlose lokale Netze die Standards IEEE802.11 und HIPPERLAN. Nur ersterer hat in der Folgezeit Verbreitung gefunden. In der mit dem Hauptantrag verteidigten Fassung legt sich das Streitpatent auf keinen dieser Standards fest.

16 b) Um eine Vielzahl unterschiedlicher Schlüssel für die symmetrische Verschlüsselung einsetzen zu können, ohne diese im Voraus auf den Endgeräten und den Zugangspunkten speichern zu müssen, sieht Merkmal 2 den Einsatz eines Identitätsmoduls vor, wie es in einem öffentlichen terrestrischen Mobilfunknetz eingesetzt wird.

17 Als Beispiel hierfür zeigt die Beschreibung ein für das GSM-Netz geeignetes SIM-Modul auf. Ein solches Modul umfasst eine Karte mit einem integrierten Schaltkreis, auf der ein geheimer Schlüssel (Ki) gespeichert ist (Abs. 14).

18 Mit Hilfe dieses Schlüssels und mehrerer vom Mobilfunk-Netzwerk übermittelter Challenge-Codes errechnet das Endgerät gemäß Merkmal 2 mehrere erste Schlüssel. Auf deren Grundlage wird gemäß Merkmal 3 ein zweiter Schlüssel errechnet, der mit Hilfe der in Merkmal 4 vorgesehenen Mittel zur Verschlüsselung und Entschlüsselung der im lokalen Netzwerk übertragenen Daten eingesetzt werden kann.

19 Nach den Ausführungen in der Beschreibung ist der zweite Schlüssel (K) schwieriger zu definieren als der erste Schlüssel (Kc). Deshalb bietet er ein höheres Maß an Sicherheit als eine GSM-Verschlüsselung (Abs. 29).

20 Für das in der Streitpatentschrift geschilderte Ausführungsbeispiel sind die Kommunikationsvorgänge zur Authentifizierung und Schlüsselberechnung in der nachfolgend wiedergegebenen Figur 2 dargestellt.

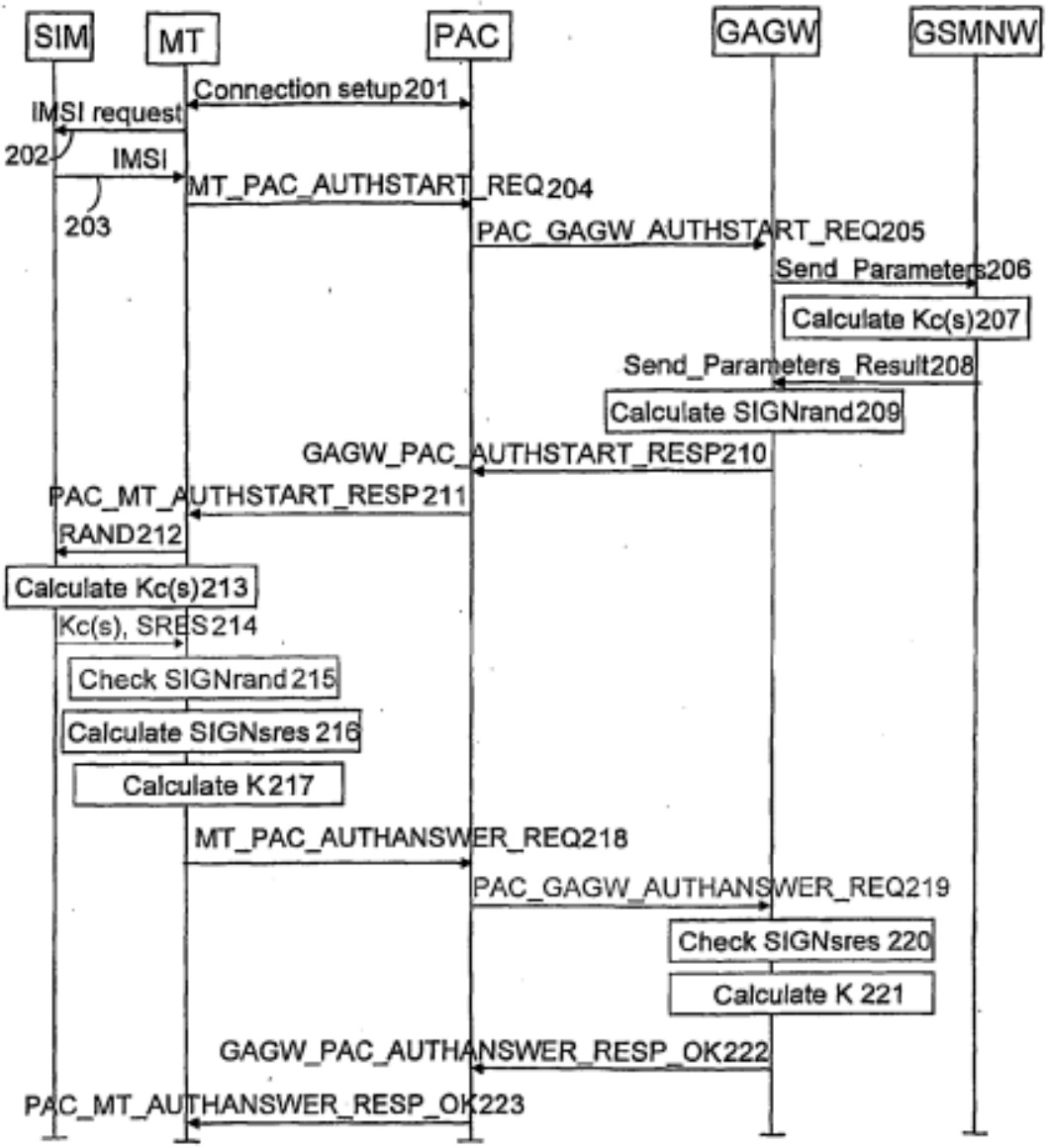


Fig. 2

21 Bei diesem Beispiel übersendet das Mobilgerät (MT) an den Zugangspunkt (PAC) in Schritt (218) zusätzlich eine Authentifizierungs-Antwort, die es ebenfalls anhand des im Identitätsmodul (SIM) gespeicherten Schlüssels (Ki) und der ihm in Schritt (211) übermittelten Challenge-Codes errechnet. Der Zugangspunkt vergleicht diese Daten zum Zwecke der Authentifizierung mit Angaben, die

ihm das Mobilfunk-Netz (GSMNW) über ein Authentifizierungs- und Abrechnungs-Gateway (GAGW) zur Verfügung gestellt hat (Abs. 30). Wenn die Prüfung positiv ausfällt, wird der zweite Schlüssel (K) zur Ver- und Entschlüsselung der Daten eingesetzt. Der Zugangspunkt erhält auch diesen Schlüssel vom Mobilfunk-Netz (Abs. 31). Er muss deshalb nicht über das lokale Netzwerk übermittelt werden.

22 c) Hinsichtlich der zwischen den Parteien umstrittenen Frage, ob der zweite Schlüssel (K) zur Verschlüsselung sämtlicher Nutzdaten im drahtlosen lokalen Netzwerk eingesetzt werden muss oder ob es ausreicht, wenn ein Teil dieser Daten verschlüsselt wird, trifft Patentanspruch 11 schon deshalb keine Festlegung, weil er kein Verfahren schützt, sondern ein Erzeugnis.

23 Entgegen der Auffassung der Klägerinnen und des Patentgerichts ist Merkmal 4 aber zu entnehmen, dass die dort vorgesehenen Verschlüsselungsmittel dazu geeignet sein müssen, alle im drahtlosen lokalen Netzwerk übertragenen Nutzdaten zu verschlüsseln. Nicht zu den Nutzdaten in diesem Sinne zählen solche Daten, die in unverschlüsselter Form benötigt werden, um die Nutzdaten vom Endgerät zum Zugangspunkt oder umgekehrt zu übertragen.

24 aa) Für dieses Verständnis spricht der Wortlaut des Merkmals 4, der Mittel zur Ver- und Entschlüsselung "der Daten" (the data) vorsieht, also grundsätzlich keine Unterscheidung zwischen einzelnen Arten von Nutzdaten trifft.

25 bb) In dieselbe Richtung deuten die Ausführungen in der Beschreibung des Streitpatents zum Verschlüsselungsstandard WEP.

26 Wie bereits oben aufgezeigt wurde, wird bereits bei der Beschreibung des Stands der Technik darauf hingewiesen, dass die Verschlüsselung in einem IEEE802.11-Netz nach dem Standard WEP auf der Schicht 2 (MAC) erfolgt (Abs. 2).

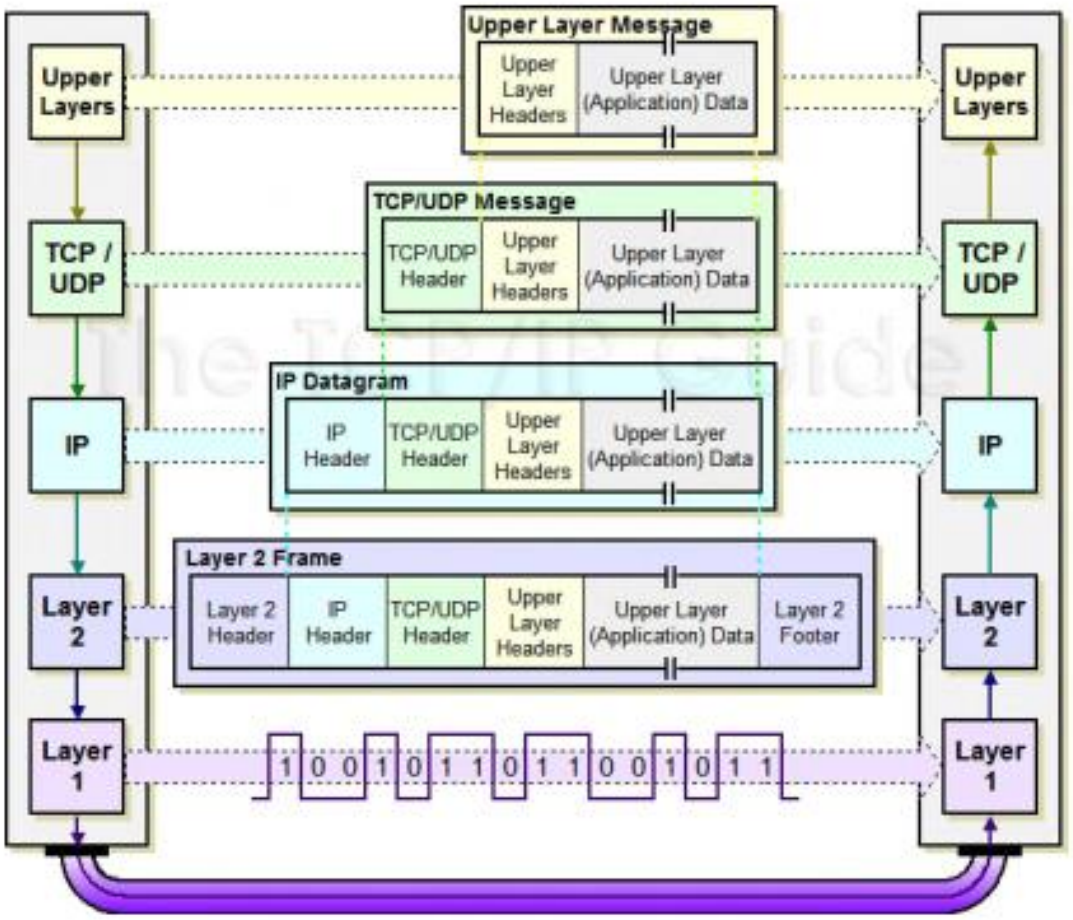
27 Bei der Schilderung des in Figur 2 dargestellten Ausführungsbeispiels wird in Einklang damit ausgeführt, der zweite Schlüssel (K) werde in der MAC-Schicht des Endgeräts angewendet; das Endgerät verschlüssele die an den Zugangspunkt (AP) zu sendenden und entschlüssele die von diesem empfangenen Daten unter Verwendung des Schlüssels (K) und des WEP-Algorithmus (Abs. 39).

28 cc) Vor diesem Hintergrund sind als "the data" im Sinne von Merkmal 4 grundsätzlich alle zwischen dem Endgerät und dem Zugangspunkt im lokalen Netzwerk übermittelten Daten anzusehen.

29 Patentanspruch 11 schreibt den Einsatz der Standards IEEE802.11 und WEP und eine Verschlüsselung in der MAC-Schicht zwar nicht zwingend vor. Er greift die in den genannten Standards vorgesehenen Vorgehensweisen aber insoweit auf, als er ebenfalls nicht zwischen einzelnen Daten differenziert.

30 dd) Entgegen der Auffassung des Patentgerichts steht dem nicht entgegen, dass bestimmte Daten unverschlüsselt übermittelt werden müssen, damit sie die empfangende Gegenstelle - also das Endgerät oder der Zugangspunkt - ordnungsgemäß empfangen, verarbeiten und weiterleiten kann.

31 Die insoweit maßgeblichen Zusammenhänge werden in dem nachfolgend wiedergegebenen, von der Beklagten eingereichten Schaubild (NB4) veranschaulicht.



32 Bei einer Übertragung in der Schicht 2 (MAC), wie sie für drahtlose lokale Netzwerke nach den Standards IEEE802.11 und HIPPERLAN vorgesehen ist, dürfen die als Layer 2 Header und Layer 2 Footer bezeichneten Steuerdaten nicht verschlüsselt werden, weil die übermittelten Daten sonst von dem Endgerät oder dem Zugangspunkt, für den sie bestimmt sind, nicht in ordnungsgemäßer Weise empfangen, verarbeitet und weitergeleitet werden können. Die dazwischen angeordneten Daten der höheren Schichten können hingegen verschlüsselt werden, weil ihr Inhalt für die Kommunikation auf der Schicht 2 nicht von Bedeutung ist.

33 Hieraus ist, wie das Patentgericht im Ansatz zutreffend angenommen hat, zwar die Schlussfolgerung zu ziehen, dass bei einer Verschlüsselung in der MAC-Schicht die zu dieser Schicht gehörenden Header und Footer nicht verschlüsselt werden dürfen. Entgegen der Auffassung des Patentgerichts ergibt sich daraus aber nicht, dass die Auswahl der Daten, für die eine Verschlüsselung möglich sein muss, beliebig ist. Die Auswahl hat sich vielmehr an dem Erfordernis einer fehlerfreien Übertragung in der Schicht zu orientieren, in der das drahtlose lokale Netzwerk arbeitet.

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

35 Ein drahtloses Endgerät nach Patentanspruch 11 sei aus der nach dem Prioritätstag veröffentlichten, aber prioritätsälteren internationalen Anmeldung WO 01/76134 (NK17) und den Technischen Spezifikationen zum DECT-Standard (ETS 200 466, July 1996, NK9a; ETS 300 175-1, October 1992, NK9b) vorbekannt. Ferner sei sie dem Fachmann, einem Ingenieur der Fachrichtung Elektro- oder Nachrichtentechnik oder Informatiker mit Hochschulabschluss, jeweils mit Erfahrung auf dem Gebiet der Mobilfunknetzwerke und lokalen Netzwerke und der Verschlüsselungstechnik, ausgehend von dem Normierungsentwurf von Haverinen et al. (GSM SIM Authentication for Mobile IP, Juni 2000, NK23) auch nahegelegt. NK23 befasse sich mit der Authentifizierung in einem mobilen IP-Netzwerk. Da die genauere Ausgestaltung des Netzwerks in NK23 offenbleibe, werde der Fachmann dieses in üblicher Weise ausbilden und insoweit etwa die internationale Anmeldung WO 00/02407 (NK11) heranziehen, die von einem ähnlichen Aufbau ausgehe. Nach K23 würden im mobilen IP-Netzwerk aus mehreren Challenge-Codes mehrere Schlüssel (Kc) berechnet und daraus ein Authentifizierungsschlüssel gebildet. Dieser sei gleichzeitig der gemeinsame Sitzungsschlüssel (shared session key). Mit diesem Fachbegriff werde ein Schlüssel bezeichnet, der für eine bestimmte Sitzung gültig sei und der Ver- und Entschlüsselung der übertragenen Daten diene.

36 III. Diese Beurteilung hält der Überprüfung im Berufungsverfahren im Ergebnis stand.

37 1. Zu Recht hat das Patentgericht den mit dem Hauptantrag verteidigten Gegenstand jedenfalls im Hinblick auf die NK23 als nicht patentfähig beurteilt.

38 a) NK23 befasst sich mit der Authentifizierung zwischen einem Knoten (mobile node) und einem Agenten (mobility agent) in einem mobilen IP-Netzwerk unter Einsatz einer GSM-SIM-Karte.

39 NK23 verfolgt das Ziel, bereits vorhandene Mechanismen und Infrastruktur von GSM-Netzen zu nutzen, um Authentifizierungsschlüssel für die Kommunikation des Knotens mit dem fremden Netz (mobile-foreign) und mit dem Heimnetz (mobile-home) zu erzeugen (S. 2). Hierzu wird der Challenge-Response-Mechanismus aus GSM genutzt, der unter anderem einen 64 bit langen Schlüssel (Kc) liefert, der zur Verschlüsselung des Verkehrs über die Luftschnittstelle vorgesehen ist (S. 3 Abs. 1). Zur Authentifizierung im mobilen IP-Netzwerk werden mehrere solche Schlüssel kombiniert, um einen längeren Schlüssel zu erhalten (S. 3 Abs. 2).

40 Der mobile Knoten versendet seine Identifikationsnummer (IMSI) an den Mobilitätsagenten (mobile agent). Dieser holt damit vom GSM-Netzwerk die für den Challenge-Response-Mechanismus erforderlichen Daten ein und führt auf dieser Grundlage den Authentifizierungsvorgang mit dem Knoten durch (S. 3 Abs. 3). Nachdem der gemeinsame Sitzungsschlüssel generiert worden ist, kann sich der Knoten bei dem Mobilitätsagenten oder über diesen (with or through the mobility agent) registrieren. Der Schlüssel kann für nachfolgende Registrierungsprozesse eingesetzt werden, hat aber eine begrenzte Gültigkeitsdauer (S. 3 Abs. 4).

41 b) NK23 nimmt den verteidigten Gegenstand von Patentanspruch 11 nicht neuheitsschädlich vorweg.

42 Zwar sind, wie sich aus der Begründung des Patentgerichts ergibt und auch die Berufung nicht in Zweifel zieht, die Merkmale 1 bis 3 offenbart. Es fehlt jedoch an einer unmittelbaren und eindeutigen Offenbarung des Merkmals 4 in der Entgegenhaltung.

43 NK23 sieht einen Einsatz des Sitzungsschlüssels zum Zwecke der Verschlüsselung nur für den Verkehr auf einem GSM-Funkkanal vor. Der Sitzungsschlüssel für das mobile IP-Netzwerk wird zwar mit den gleichen Mechanismen erzeugt. Dass er zur Verschlüsselung zwischen dem Knoten und dem Zugangspunkt des lokalen Netzwerks eingesetzt wird, ist aber nicht erwähnt. Unmittelbar und eindeutig offenbart ist allein, den Sitzungsschlüssel innerhalb seiner Gültigkeitsdauer bei einer Registrierung des mobilen Knotens als Authentifizierungsmittel zu verwenden (S. 3 Abs. 3 letzter Satz und Abs. 4).

44 c) Den Sitzungsschlüssel, der für die Authentifizierung des Knotens im mobilen IP-Netzwerk verwendet wird, auch für die Verschlüsselung der Daten einzusetzen, war jedoch naheliegend.

45 aa) Ausgehend von dem Problem, eine sichere Datenverschlüsselung in drahtlosen lokalen Netzen auch für Endgeräte, die sich in verschiedenen Netzen bewegen, auf einfache Weise zu ermöglichen, bestand aus fachlicher Sicht Veranlassung, sich mit der Bereitstellung von Schlüsseln in drahtlosen lokalen Netzwerken zu befassen.

46 Wie aus der Beschreibung des Streitpatents hervorgeht und auch die Berufung nicht in Zweifel zieht, waren im Stand der Technik Verfahren zur Verschlüsselung des Datenverkehrs zwischen einem Endgerät und dem Zugangspunkt eines drahtlosen lokalen Netzwerks bekannt. Wie auch in NK11 (S. 2 Z. 9-19) ausgeführt wird, gestaltete es sich bei der Anwendung solcher Verfahren als schwierig, die dafür erforderlichen Schlüssel zu verwalten. Insbesondere

fehlte es, wie auch die Streitpatentschrift darlegt (Abs. 3), in manchen Situationen an einer praktikablen Möglichkeit, die Schlüssel vorab in den an der Kommunikation beteiligten Geräten zu hinterlegen. Deshalb bestand Anlass, nach geeigneten Lösungen zu suchen, um dieses Problem zu überwinden.

47 bb) Bei der Suche nach solchen Lösungen bestand Veranlassung, auch Stand der Technik in den Blick zu nehmen, der sich mit Schlüsseln befasst, die zur Authentifizierung zwischen einem Endgerät und einem mobilen IP-Netzwerk verwendet werden.

48 Das genannte Problem der Erzeugung und sicheren Bereitstellung von Schlüsseln stellte sich unabhängig davon, ob die Schlüssel zur Authentifizierung oder zur Verschlüsselung eingesetzt werden. Umgekehrt war bekannt, dass die Durchführung eines vorbekannten Authentifizierungs- oder Verschlüsselungsverfahrens nicht davon abhängt, auf welche Weise ein hierfür geeigneter Schlüssel erzeugt und den an der Kommunikation beteiligten Geräten bekannt gemacht worden ist.

49 cc) Vor diesem Hintergrund bot sich die in NK23 offenbarte Vorgehensweise auch für die Erzeugung und Verteilung von Sitzungsschlüsseln zur Verschlüsselung in einem drahtlosen lokalen Netzwerk an.

50 Dies gilt umso mehr, als NK23 ausdrücklich betont, nur das Problem der Schlüsselerzeugung und -verteilung im Detail zu behandeln, und wegen aller übrigen Fragen auf bekannte Vorgehensweisen verweist.

51 NK23 setzt den Aufbau und die Funktionsweise eines GSM-Netzes und eines mobilen IP-Netzwerkes voraus und beschränkt sich auf den Vorschlag eines Protokolls für den Datenaustausch zwischen einem mobilen Knoten und einem Mobilitätsagenten (NK23, S. 2 unten). Dies gab Anlass, zur näheren Ausgestaltung auf bekannte Vorbilder für mobile IP-Netzwerke zurückzugreifen. Zu die-

sen gehörte, wie das Patentgericht zutreffend ausgeführt hat, ein drahtloses lokales Netzwerk mit einem Zugangspunkt im Sinne von Merkmal 1, wie es etwa in NK11 offenbart ist.

52 dd) Von diesem Ausgangspunkt aus bestand Anlass, den in NK23 offenbarten Gedanken, die im GSM-Standard bereits zur Verfügung stehenden Mechanismen zur Erzeugung und Bereitstellung von Schlüsseln heranzuziehen, die in anderen Netzen Einsatz finden, auch für drahtlose lokale Netzwerke nutzbar zu machen. Hierbei war es aus den bereits oben dargelegten Gründen auch naheliegend, einen so erzeugten und bereitgestellten Schlüssel nicht nur zur Authentifizierung einzusetzen, sondern auch zur Verschlüsselung der Daten innerhalb des lokalen Netzwerks, zumal NK23 ausdrücklich darauf hinweist, dass die mit Hilfe einer SIM-Karte erzeugten Schlüssel in GSM-Netzen auch zur Verschlüsselung des Datenverkehrs eingesetzt werden (Abs. 1).

53 Für die Datenverschlüsselung in drahtlosen lokalen Netzwerken geeignete Verfahren standen zur Verfügung. Dass deren Anwendung unter Einsatz eines nach dem Vorbild von K23 berechneten Schlüssels besondere Probleme aufgeworfen hätte, ist weder geltend gemacht noch sonst ersichtlich. Auch das Streitpatent greift bei dem in der Beschreibung geschilderten Ausführungsbeispiel auf den Stand der Technik zurück, und zwar in Gestalt des Verschlüsselungsverfahrens WEP (Abs. 39).

54 ee) Mit der Nutzung von WEP ist zugleich Merkmal 4 verwirklicht.

55 Wie auch die Streitpatentschrift ausführt (Abs. 2), verschlüsselt dieses Verfahren den Verkehr auf der Schicht 2 (MAC).

56 2. Ob der Gegenstand von Patentanspruch 11 durch NK17 vorweggenommen wird, bedarf angesichts dessen keiner Entscheidung.

57 IV. Die mit den Hilfsanträgen verteidigten Gegenstände sind ebenfalls nicht patentfähig.

58 1. Ausgehend von NK23 war, wie das Patentgericht zutreffend und insoweit unbeanstandet ausgeführt hat, der Einsatz eines drahtlosen lokalen Netzwerks nach den im Stand der Technik bekannten Standards IEEE802.11 und HIPERLAN nahegelegt.

59 2. Das gemäß Hilfsantrag 3 zusätzlich vorgesehene Merkmal, wonach auf der MAC-Schicht ein Verfahren für den Mehrfachzugriff mit Trägerprüfung und Kollisionsvermeidung CSMA/CA verwendet wird, ist ausgehend von NK23 ebenfalls nahegelegt.

60 Nach den insoweit nicht angegriffenen Feststellungen des Patentgerichts sah der Standard IEEE802.11 bereits im Prioritätszeitpunkt den Einsatz eines solchen Verfahrens vor. Die Heranziehung dieses Standards war aus den bereits zu Hilfsantrag 2 dargelegten Gründen nahegelegt.

61 3. Entsprechendes gilt für Hilfsantrag 4, der sich von der Fassung des zweitinstanzlichen Hauptantrags allein darin unterscheidet, dass das drahtlose lokale Netzwerk dem Standard IEEE802.11 entspricht.

62 V. Die Kostenentscheidung beruht auf § 121 Abs. 2 PatG in Verbindung mit § 97 Abs. 1 ZPO.

Bacher Grabinski Hoffmann

Kober-Dehm Rensen

Vorinstanz:
Bundespatentgericht, Entscheidung vom 24.01.2019 - 2 Ni 5/17 (EP)