BUNDESPATENTGERICHT

L e i t s a t z

Aktenzeichen:	2 Ni 5/17 (EP) verbunden mit 2 Ni 12/17 (EP) und 2 Ni 13/17 (EP)
Entscheidungsdatum:	24. Januar 2019
Rechtsbeschwerde zugelassen:	nein
Normen:	§ 83 Abs. 4 Satz 1 Nr. 2 PatG; § 83 Abs. 4 Satz 1 Nr. 2 PatG

„Datenchiffrierung in einem drahtlosen Telekommunikationssystem“

1. Die Verteidigung durch Hilfsanträge nach Ablauf der im qualifizierten Hinweis gesetzten Frist in der mündlichen Verhandlung kann zurückgewiesen werden, wenn diese Hilfsanträge keine Reaktion auf den Verlauf der mündlichen Verhandlung darstellen und der Klägerpartei eine sachgerechte Auseinandersetzung mit den Hilfsanträgen in der mündlichen Verhandlung nicht zuzumuten ist.

2. Für eine unter dem Gesichtspunkt des rechtlichen Gehörs erforderliche sachgerechte Auseinandersetzung mit Hilfsanträgen, die nach der Mittagspause in der mündlichen Verhandlung eingereicht werden und eine neue Verteidigungslinie darstellen, reicht die Zeit bis zum Beginn des Folgetermins am Vormittag des nächsten Tages in der Regel nicht aus.

3. Für eine Entschuldigung der Verspätung ihres Vorbringens im Sinne des § 83 Abs. 4 Satz 1 Nr. 2 PatG genügt es nicht, wenn die Beklagte behauptet, eine von der Klägerin erst kurz vor der mündlichen Verhandlung erstmals thematisierte technische Problematik sei ihr vorher nicht klar gewesen, sofern die Beklagte bereits aufgrund des Inhalts des qualifizierten Hinweises des Senats Anlass und ausreichend Zeit hatte, die betreffende Problematik zu erkennen und auf sie einzugehen.

BUNDESPATENTGERICHT

IM NAMEN DES VOLKES

URTEIL

2 Ni 5/17 (EP)
verbunden mit
2 Ni 12/17 (EP)
und
2 Ni 13/17 (EP)

(Aktenzeichen)

Verkündet am
24. Januar 2019
…

In der Patentnichtigkeitssache

…

ECLI:DE:BPatG:2019:240119U2Ni5.17EP.0

...

…

betreffend das europäische Patent 1 304 002
(DE 601 32 591)

hat der 2. Senat (Nichtigkeitssenat) des Bundespatentgerichts auf Grund der mündlichen Verhandlung vom 24. Januar 2019 unter Mitwirkung des Vorsitzenden Richters Guth sowie der Richter Dipl.-Phys. Dr. rer. nat. Friedrich, Dipl.-Phys. Dr. rer. nat. Zebisch, Dr. Himmelmann und Dr.-Ing. Kapels für Recht erkannt:

I. Das europäische Patent 1 304 002 wird im Umfang seines Patentanspruchs 11 mit Wirkung für das Hoheitsgebiet der Bundesrepublik Deutschland für nichtig erklärt.

II. Die Kosten des Rechtsstreits trägt die Beklagte.

III. Das Urteil ist gegen Sicherheitsleistung in Höhe von 120 % des zu vollstreckenden Betrages vorläufig vollstreckbar.

T a t b e s t a n d

Die Beklagte ist Inhaberin des auch mit Wirkung für die Bundesrepublik Deutschland erteilten und am 28. Juni 2001 in der Verfahrenssprache Englisch international angemeldeten europäischen Patents 1 304 002 mit der Bezeichnung „ARRANGING DATA CIPHERING IN A WIRELESS TELECOMMUNICATION SYSTEM“ (deutsch: ARRANGIEREN DER DATENCHIFFRIERUNG IN EINEM DRAHTLOSEN TELEKOMMUNIKATIONSSYSTEM), das die Priorität der Voranmeldung FI 20001567 vom 30. Juni 2000 in Anspruch nimmt. Das Patent wird vom Deutschen Patent- und Markenamt unter der Nummer DE 601 32 591 geführt. Der Veröffentlichungstag der mit der EP 1 304 002 B1 (Streitpatentschrift) publizierten Patenterteilung ist der 23. Januar 2008. Die dem Streitpatent zugrundeliegende internationale Anmeldung wurde am 10. Januar 2002 mit der WO 2002/003730 A1 offengelegt.

Das Streitpatent umfasst 15 Patentansprüche, von denen die vier nebengeordneten Ansprüche 1, 8, 11 und 14 jeweils auf ein Verfahren, ein Telekommunikationssystem, ein drahtloses Endgerät und einen Zugangspunkt gerichtet sind, und die abhängigen Ansprüche 2 bis 7, 9 und 10, 12 und 13 sowie 15 direkt oder indirekt auf die jeweiligen unabhängigen Ansprüche rückbezogen sind.

Die H… GmbH in D…, hat am
15. Januar 2016 in der Patentnichtigkeitssache mit dem Aktenzeichen 2 Ni 6/17 (EP) Klage vor dem Bundespatentgericht gegen den deutschen Teil des Streitpatents erhoben und beantragt, das Streitpatent mit Wirkung für das Hoheitsgebiet der Bundesrepublik Deutschland in vollem Umfang für nichtig zu erklären. Sie hat mit Schriftsatz vom 2. November 2018 ihre Nichtigkeitsklage zurückgenommen. Der Senat hat am 6. November 2018 beschlossen, die Verbindung der Verfahren 2 Ni 5/17 (EP) mit den Verfahren 2 Ni 6/17 (EP), 2 Ni 12/17 (EP) und 2 Ni 13/17 (EP) bezüglich des Verfahrens 2 Ni 6/17 (EP) aufzuheben.

Mit ihren Klagen begehren die verbliebenen Klägerinnen jeweils die Nichtigerklärung des deutschen Teils des europäischen Patents im Umfang seines Anspruchs 11.

Patentanspruch 11 lautet in der englischen Fassung gemäß EP 1 304 002 B1:

> „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.“

Die Klägerinnen machen die Nichtigkeitsgründe der mangelnden Ausführbarkeit (nicht die Klägerin zu 1) und der fehlenden Patentfähigkeit geltend.

Zur Stützung ihres Vorbringens nennt die Klägerin zu 1 u.a. folgende Druckschriften:

BDP-1EP	EP 1 304 002 B1 (Streitpatentschrift)
BDP-1DE	DE 601 32 591 T2 (deutsche Übersetzung des Streitpatents)
BDP-1WO	WO 2002/003730 A1 (Offenlegungsschrift des Streitpatents)
BDP-2	DPMA Registerauszug zum Streitpatent
NiK-1	WO 00/76194 A1
NiK-2	UMTS Standard ETSI TS 133 102 V3.4.0 (2000-03)
NiK-3	GSM Standard ETSI TS 100 929 V6.1.0 (1999.07)
NiK-4	DE 196 30 920 C1
NiK-5	WO 01/76134 A1
NiK-5prio	englische Übersetzung der finnischen Voranmeldung 20000760 bzw. PCT/FI01/00015 zur NiK-5

Die Klägerin zu 1 ist der Ansicht, der Gegenstand des angegriffenen Anspruchs 11 sei nicht neu jeweils gegenüber den nur unter dem Aspekt der Neuheit zu berücksichtigenden nach dem Prioritätszeitpunkt veröffentlichten älteren Anmeldungen NiK-1 und NiK-5. Außerdem beruhe Anspruch 11 des Streitpatents nicht auf einer erfinderischen Tätigkeit, weil Anspruch 11 sich für den Fachmann durch die Druckschrift NiK-2 sowie durch die Druckschrift NiK-4 in Verbindung mit der Druckschrift NiK-3 aus dem Stand der Technik ergebe und deshalb nahegelegt sei.

Zur Stützung ihres Vorbringens nennt die Klägerin zu 2 u. a. folgende Druckschriften:

N1	EP 1 304 002 B1 (Streitpatentschrift)
N2	DPMA Registerauszug vom 10. Mai 2016 zum Streitpatent
N3	WO 2002/003730 A1 (Offenlegungsschrift des Streitpatents)
N4	Klageschrift im Verletzungsprozess vor dem Landgericht Mannheim
N5	Merkmalsanalyse des erteilten Anspruchs 11
N6	Merkmalsanalyse des geänderten Anspruchs 11
N7, N8	Triplik der Klägerin im Verletzungsverfahren vom 14. Februar 2017
N9	Replik der Klägerin im Verletzungsverfahren vom 12. August 2016
N10	Sachverständigengutachten von Prof. W…
N11	Quintuplik vom 14.Juli 2017 im parallelen Verletzungsverfahren mit dem Az. 2 O 18/16 (in Auszügen)
N12	Merkmalsanalyse des geänderten Anspruchs 11 im parallelen Verletzungsverfahren gemäß dem Hauptantrag
N13	Merkmalsanalyse des geänderten Anspruchs 11 im parallelen Verletzungsverfahren gemäß dem Hilfsantrag 1
N14	Merkmalsanalyse des geänderten Anspruchs 11 im parallelen Verletzungsverfahren gemäß dem Hilfsantrag 2

NK1	EP 1 103 137 B1
NK1_DE	Übersetzung der NK1
NK2	John Scourias; Overview of GSM: The Global System for Mobile Communication; University of Waterloo, 13. März 1996
NK3	EP 0 955 783 A2
NK4	TSGS-WG3#4(99)xxx, TSG-SA WG3 (Security) meeting #4, London, 16--18. Juni 1999
NK5	EP 0 930 795 A1
NK6	Michel Mouly, Marie-Bernadette Pautet; The GSM System for Mobile Communications; Chapter 7.2 Security Management, S. 477-492, 1992, ISBN 2-9507190-0-7
NK7	Bernard Adoba et al.; Präsentation: IEEE 802.1X For Wireless LANs, IEEE 802.11-00/035, März 2000
NK8	US 5 539 824 A
NK9	DECT-Standard, insbesondere
NK9a	ETSI European Telecommunication Standard ETS 300 466 - DE/RES-03048 (Juli 1996)
NK9a_DE	Übersetzung der NK9a
NK9a1	ETSI European Telecommunication Standard ETS 300 370 - DE/RES-03017 (Juli 1995)
NK9a1_DE	Übersetzung der NK9a1
NK9b	ETSI European Telecommunication Standard ETS 300 175-1 - DE/RES-3001-1 (Oktober 1992)
NK9b_DE	Teilübersetzung der NK9b
NK9c	ETSI European Telecommunication Standard ETS 300 534 - GSM 03.20 (September 1994)
NK9d	ETSI European Telecommunication Standard ETS 300 509 - GSM 02.17 (September 1994)
NK9e	ETSI EN 300 175-7 V1.4.2 (1999-06) Digital Enhanced Cordles Telecommunications (DECT); Common Interface (CI); Part 7: Security features

NK9f ETSI Technical Report ETR 178, January 1997, Second Edition; Digital Enhanced Cordless Telecommunications (DECT); A high level guide to the DECT standardization

NK11 WO 00/02407 A2

NK12 IEEE Standard 802.11 (1997)

NK13 P. T. Davis und C. R. McGuffin Wireless Local Area Networks, 1995

NK14 Ch. Lüders; Lokale Funknetze - Wireless LANs (IEEE 802.11), Bluetooth, DECT, Vogel Industries Medien GmbH & Co. KG, Würzburg, 2007, S. 7-23, 198, 199, 280-283

NK14a Seiten 190, 191, 534, 535 der NK14

NK15 R. Bräuer, G. Arens und P. Zimmers; Alles über schnurlose Telefone und Nebenstellenanlagen, Franzis-Verlag GmbH, Poing, 1995, S. 5-9, 61-65

NK16 Z. Zvonar, P. Jung, K. Kammerlander; GSM-Evolution Towards 3rd Generation Systems, Kluwer Academic Publishers, Dordrecht, 1999, S. 283-299

NK17 WO 01/76134 A1

NK17a DE 601 14 789 T2 (erteilte deutsche Fassung der NK17)

NK18 D. Harkins, D. Carrel, cisco Systems, November 1998, Network Working Group Request for Comments: 2409; RFC2409

NK18a Deutsche Übersetzung der NK18

NK19 Thomas F. La Porta, Luca Salgarelli, Gerard T. Foster; Mobile IP and Wide Area Wirelesse Data, IEEE 1998

NK20 Roman Pichna, Tero Ojanperä, Harri Posti, Jouni Karppinen; Wireless Internet - IMT-2000/Wireless LAN Interworking; IN: Journal of Communications and Networks, Vol. 2, No. 1, March 2000, S. 46-57

NK21 N. Asokan, Nokia Research Center: Präsentation: Security Issues in Mobile Communication Systems, IAB workshop on wireless internetworking, February 29 - March 2, 2000

NK21a IAB Wireless Internetworking Workshop 2000, Webseitenauszug

NK22	Seiten 534 und 535 aus dem Fachbuch „Handbook of Internet and Multimedia Systems and Applications”, veröffentlicht 1998
NK23	H. Haverinen Nokia Mobile IP Working Group Internet Draft, GSM SIM Authentication for Mobile IP, June 2000
NK23_DE	Übersetzung der NK23
NK23a	S. Bradner, Harvard University, Network Working Group Request for Comments: 2026; RFC2026, The Internet Standards Process - Revision 3, October 1996
NK23b	Kopie einer bei IETF archivierten E-Mail vom 20.Juni 2000 als Veröffentlichungsnachweis für die Druckschrift NK23
NK23c	Webseitenauszug, https://web.archive.org/web/20000815200849/http://www.ietf.org/internet-drafts/
NK23d	Webseitenauszug: „datatracker.ietf.org/doc/draft-haverinen-mobileip-gsmsim/history“
NK24	Chii-Hwa Lee, Min-Shiang Hwang, Wei-Pang Yang; Enhanced privacy and authentication for the global system for mobile communications; IN: Wireless Networks 5 (1999), S. 231-243
NK24_DE	Übersetzung der NK24
NK25	US 5 544 245 A
NK26	Jochen Schiller; Mobile Communications, Addison-Wesley, Pearson Education Limited, Harlow, 2000, S. 84, 167
NK27	EP 0 998 094 A2

Die Klägerin zu 2 meint, Anspruch 11 sei nicht neu jeweils gegenüber den Druckschriften NK1, NK9a, der NK11 und NK19 und beruhe nicht auf einer erfinderischen Tätigkeit gegenüber der Druckschrift NK3 allein oder in Verbindung mit der Druckschrift NK5, gegenüber der Druckschrift NK4 allein oder in Verbindung mit einer den Druckschriften NK2 oder NK6, gegenüber der Druckschrift NK20 in Verbindung mit der Druckschrift NK6, gegenüber der Druckschrift NK9 in Verbindung mit den Druckschriften NK23 oder NK24 und gegenüber der Druckschrift NK23 alleine.

Zur Stützung ihres Vorbringens nennt die Klägerin zu 3 u. a. folgende Druckschriften:

MN1	Klageschrift der H… GmbH vom 15. Januar 2016 (2 Ni 6/17 (EP)
MN1a	Anlagen aus dem Nichtigkeitsverfahren 2 Ni 6/17 (EP)
MN2	Klageschrift aus dem Verletzungsverfahren vom 26. Januar 2016
MN3	Druckschriften NK9 bis NK12 aus dem Verfahren 2 Ni 6/17 (EP
MN4a,b	Merkmalsgliederung des erteilten Anspruchs 11 in englischer und deutscher Fassung
MN5	Wikipedia-Ausdruck zum Internet Explorer 2
MN6	Triplik aus dem Verletzungsverfahren

und die NK-Dokumente aus den Patentnichtigkeitssachen 2 Ni 6/17 (EP) und 2 Ni 12/17 (EP). Zur Liste der NK-Dokumente aus der Patentnichtigkeitssache 2 Ni 6/17 (EP) sei auf die Liste der Druckschriften der Klägerin zu 2 verwiesen, die abgesehen von wenigen Bezeichnungen gleich ist. Zusätzlich hat die Klägerin zu 3 in der mündlichen Verhandlung das folgende Dokument vorgelegt:

NK28	Buchauszug, The GSM System, Mobility and Security Management, Kap. 7.2 Security Management, S. 477-492 (vgl. Anlange NK6)

Die Klägerin zu 3 ist der Meinung, Anspruch 11 sei nicht neu jeweils gegenüber den Druckschriften NK9 und NK11. Sie stützt sich (zuletzt) vor allem auf die Druckschrift NK17 bzw. das Prioritätsdokument NiK-5prio, die Druckschrift NK9 mit den Anlagen NK9a, NK9b und NK9c, sowie auf die Druckschrift NK23 in Verbindung mit dem durch die Druckschriften NK11 und NK20 sowie NK24 belegten Fachwissen.

Die Klägerinnen stellen jeweils den Antrag,

> das europäische Patent 1 304 002 im Umfang seines Anspruchs 11 mit Wirkung für das Hoheitsgebiet der Bundesrepublik Deutschland für nichtig zu erklären.

Die Beklagte stellt den Antrag,

> die Klagen abzuweisen,
> hilfsweise
> das europäische Patent 1 304 002 dadurch teilweise für nichtig zu erklären, dass sein Patentanspruch 11 die Fassung eines der Hilfsanträge 1 bis 4 vom 21. August 2018, in dieser Reihenfolge, erhält,

macht weiterhin die in der mündlichen Verhandlung um 13:25 Uhr überreichten

> Hilfsanträge 0a und 0b jeweils vom 24. Januar 2019 zum Gegenstand ihrer Antragstellung

und beantragt außerdem,

> dass die dort handschriftlich eingefügten Änderungen jeweils auch in den Text der bereits gestellten Hilfsanträge entsprechend eingefügt werden und diesen jeweils als zusätzliche Hilfsanträge a und b folgen sollen.

Die Beklagte tritt der Argumentation der Klägerinnen in allen wesentlichen Punkten entgegen und verweist zur Stützung ihres Vorbringens u. a. auf folgende Dokumente:

NB1	WO 00/76194 A1 als Offenlegungsschrift der NK1, da nur diese eine ältere Anmeldung ist
NB2	Gutachten von Univ.-Prof. Dr.-Ing. habil. S… betreffend Schlüsselgenerierung und –austausch bei IEEE 802.11, DECT und GSM in Bezug auf EP 1 304 002

NB3 bearbeitete Fig. 1 der NK11

NB4 Schaubild zum OSI-Schichtmodell

NB5 Dr. habil. Claudi Eckert; IT-Sicherheit, Konzepte – Verfahren - Protokolle, Oldenbourg Verlag München Wien 2001, S. 470-479

NB6 Ausdruck der Internetseite des Bundesamts für Sicherheit in der Informationstechnik; M 4.90 Einsatz von kryptographischen Verfahren auf den verschiedenen Schichten des ISO/OSI-Referenzmodells

Zudem überreicht sie in der mündlichen Verhandlung das Dokument

NB7 Diplomarbeit von Christine Reckziegel (Hochschule Bremen) mit dem Titel „Analysis and Assessment of Secure Mechanisms for the Building of a Secure Server Network - Cryptographic Systems and Applications, in particular Virtual Private Networks -“ vom 31. Mai 1999.

Ihrer Auffassung nach wiesen weder die Figuren noch die Beschreibung der NK17 und der NiK-5prio alle Merkmale des Anspruchs 11 auf, so dass dieser neu gegenüber der nachveröffentlichten Druckschrift NK17 sei.

Dies gelte auch gegenüber den DECT-Standarddokumenten NK9a in Verbindung mit NK9b und NK9c, da auch sie nicht alle Merkmale des Anspruchs 11 offenbarten.

Zudem beruhe der Gegenstand des Patentanspruchs 11 auf einer erfinderischen Tätigkeit, denn die Druckschrift NK23 führe weder allein noch in Zusammenschau mit der Druckschrift NK11 zum Gegenstand des Anspruchs 11. Außerdem werde bestritten, dass die Druckschrift NK23 zum vorveröffentlichten Stand der Technik gehöre.

Daher sei das Streitpatent in der erteilten Fassung bestandsfähig, insbesondere aber in der Fassung der Hilfsanträge, in denen die geäußerten Bedenken berücksichtigt worden seien.

Wegen der weiteren Einzelheiten wird auf den Akteninhalt verwiesen.

E n t s c h e i d u n g s g r ü n d e

Die Klage, mit der u. a. der Nichtigkeitsgrund der fehlenden Patentfähigkeit (Art. II § 6 Abs. 1 Nr. 1 IntPatÜG, Art. 138 Abs. 1 lit. a) EPÜ i. V. m. Art. 54 Abs. 1 bis 3 und Art. 56 EPÜ) geltend gemacht wird, ist zulässig.

Sie ist auch begründet. Das Streitpatent hat weder in der erteilten Fassung nach Hauptantrag noch in der Fassung eines der Hilfsanträge Bestand, da dem Gegenstand des Patents in der Fassung des Hauptantrags und der Hilfsanträge 1 bis 4 der Nichtigkeitsgrund der fehlenden Patentfähigkeit entgegensteht.

Denn die nur hinsichtlich der Neuheit relevante nachveröffentlichte ältere Anmeldung NK17 offenbart auch unter Berücksichtigung des Offenbarungsgehalts des Prioritätsdokuments NiK-5prio ein drahtloses Endgerät mit sämtlichen Merkmalen des Anspruchs 11 nach Hauptantrag und nach den Hilfsanträgen 1 und 2.

Zudem legt das vorveröffentlichte Dokument NK23 i. V. m. dem durch die Druckschriften NK11 und NK20 belegten Fachwissen dem Fachmann ein drahtloses Endgerät mit sämtlichen Merkmalen des Anspruchs 11 nach Hauptantrag und nach den Hilfsanträgen 1 bis 4 nahe.

Auch hinsichtlich des Dokuments NK9 mit den Anlagen NK9a, NK9b und NK9c ist das drahtlose Endgerät des mit Hauptantrag verteidigten erteilten Anspruchs 11 wegen fehlender Neuheit nicht patentfähig.

I.

1. Das Streitpatent betrifft das Einrichten einer Datenverschlüsselung in drahtlosen Telekommunikationssystemen, insbesondere in drahtlosen lokalen Netzen *(Wireless Local Area Networks, WLANs)*.

Solche drahtlosen lokalen Netze seien nach den Ausführungen im Streitpatent zum Prioritätszeitpunkt in verstärktem Maß zusätzlich zu den sog. öffentlichen landgebundenen Mobilnetzen, bspw. dem GSM- oder UMTS-Netz eingerichtet worden, und sie würden bspw. auf dem IEEE802.11-Standard basieren. Der Sicherheit von IEEE802.11-Netzen sei durch das Erzeugen einer WEP (Wired Equivalent Privacy) Funktion besondere Aufmerksamkeit gewidmet worden, wobei die WEP Funktion auf einem symmetrischen Algorithmus basiere, bei dem für das Ver- und Entschlüsseln von Daten derselbe Verschlüsselungsschlüssel verwendet werde.

Bei einigen drahtlosen Telekommunikationsnetzwerken wie IEEE802.11 WLAN-Netzen sei es aber problematisch, dass diese Schlüssel vorab im Endgerät und im Zugangspunkt gespeichert sein müssten. Wenn das Endgerät und das Netz nicht über denselben Schlüssel verfügen würden, könnten die Daten zwischen dem Netz und dem Endgerät nicht verschlüsselt werden. Auch sei es schwierig, verschiedene Verschlüsselungsschlüssel hinzuzufügen, und eine sichere Datenübertragung könne nicht immer für Endgeräte angeboten werden, die sich in verschiedenen Netzen bewegten / *vgl. Abs. [0001] bis [0003] des Streitpatents.*

Vor diesem Hintergrund liegt dem Streitpatent als technisches Problem die Aufgabe zugrunde, ein Verfahren zur Verfügung zu stellen, nach dem Schlüssel zur Verschlüsselung in einem drahtlosen lokalen Netz (WLAN) erzeugt und eingesetzt werden, um die oben genannten Probleme zu vermeiden / *vgl. Abs. [0006] des Streitpatents.*

2. Hinsichtlich der Definition des Fachmanns hat die Beklagte, zuletzt in ihrer Eingabe vom 15. November 2018, unter Verweis auf Abs. [0006] des Streitpatents vorgetragen, dass die technische Aufgabe des Streitpatents darin bestehe, ein Verfahren zur Verfügung zu stellen, nach dem Schlüssel zur Verschlüsselung in einem WLAN erzeugt und eingesetzt werden. Der zuständige Fachmann sei daher ein Ingenieur der Fachrichtung Elektro- oder Nachrichtentechnik oder ein Informatiker mit Hochschulabschluss und mehrjähriger Erfahrung in der Verschlüsselungstechnologie, der jedoch dahingehend einschränkend zu definieren sei, dass er vor allem Erfahrung mit lokalen Netzwerken habe und auch nur in dieser Hinsicht an Standardisierungsprozessen und Arbeitsgruppen beteiligt sei. Insbesondere seien bei der Definition des Fachmanns die unterschiedlichen Denkwelten von Mobilfunk einerseits sowie WLAN andererseits zu berücksichtigen, wobei aufgrund der Komplexität dieser beiden Welten, die sich bereits an der ausufernden Menge von Standardisierungsdokumenten für die beiden Netzwerktypen zeige, Fachleute auf dem Gebiet der Mobilfunknetzwerke nicht auch noch vertiefte Kenntnisse über WLAN und umgekehrt haben könnten, geschweige denn aktiv an der Standardisierung dieser beiden Netzwerktypen hätten mitarbeiten können.

Dieser einschränkenden Definition des Fachmanns konnte sich der Senat nicht anschließen. Denn nach der Rechtsprechung des Bundesgerichtshofs (BGH, Urteil vom 9. Januar 2018 – X ZR 14/16 – Leitsatz, GRUR 2018, 390, Rn. 31 – Wärmeenergieverwaltung) dient die Definition des Fachmanns dazu, eine fiktive Person festzulegen, aus deren Sicht das Patent und der Stand der Technik zu würdigen sind. Da das Streitpatent und der Stand der Technik sowohl lokale Netzwerke als auch Mobilfunknetzwerke betreffen, ist als hier zuständiger Fachmann folglich ein berufserfahrener Ingenieur der Fachrichtung Elektro- oder Nachrichtentechnik oder ein Informatiker mit Hochschulabschluss und mehrjähriger Erfahrung in der Verschlüsselungstechnik drahtloser Telekommunikationsnetze zu definieren, der an Standardisierungsprozessen und Arbeitsgruppentreffen beteiligt ist und über eigene Erfahrung auf dem Gebiet der Mobilfunknetzwerke und lokalen Netzwerke verfügt und sich als Teil eines Teams ggf. mit Fachleuten auf diesen Fachgebieten austauscht.

Entgegen den Ausführungen der Beklagten und der im Gutachten NB2 vertretenen Meinung stellen Mobilfunk einerseits und WLAN andererseits auch keine unterschiedlichen Denkwelten dar, deren Fachleute nur auf jeweils einem der beiden Gebiete vertiefte Kenntnisse haben, denn wie bereits das Standardisierungsdokument NK9a zeigt, dessen Titelblatt auf DECT als Beispiel eines drahtlosen, lokalen Netzwerks und auf GSM als Beispiel eines öffentlichen landgestützten Mobilnetzes verweist und in dessen Kapiteln 1 und 2 auf das Zusammenspiel lokaler und mobiler Netze und die zugehörigen Standardisierungsdokumente hingewiesen wird, besteht eine enge Verbindung zwischen lokalen und mobilen Netzen, die sich in den entsprechenden Standardisierungsdokumenten widerspiegelt, weshalb die daran beteiligten Fachleute als Teil eines Teams auch über vertiefte Kenntnisse auf beiden Gebieten verfügen.

3. Gemäß den erteilten Ansprüchen nach **Hauptantrag** wird die Aufgabe durch die Gegenstände der unabhängigen Ansprüche 1, 8, 11 und 14 gelöst, die ein Verfahren zum Einrichten von Datenverschlüsselung in einem Telekommunikationssystem (Anspruch 1), ein Telekommunikationssystem (Anspruch 8), ein drahtloses Endgerät (Anspruch 11) und einen Zugangspunkt für ein drahtloses lokales Netzwerk (Anspruch 14) betreffen.

Der von den Nichtigkeitsklägerinnen angegriffene erteilte Anspruch 11 hat unter Behebung eines offensichtlichen Fehlers („einem“ statt „dem“) und mit einer Merkmalsgliederung versehen auf Deutsch folgenden Wortlaut:

Hauptantrag (erteilter Anspruch 11):

11 Drahtloses Endgerät, umfassend

11.1 einen Sende-Empfänger zum Aufbauen einer drahtlosen Verbindung mit einem Zugangspunkt in einem drahtlosen, lokalen Netzwerk und

11.2 ein Identitätsmodul zum Berechnen (213) von mindestens einem ersten Verschlüsselungsschlüssel gemäß ~~dem~~ einem öffentlichen landgestützten Mobilnetz unter Verwendung eines Geheimschlüssels, welcher in dem Identitätsmodul gespeichert ist, und mindestens einem Challenge-Code, welcher von dem Mobilnetzwerk gesendet wird,
dadurch gekennzeichnet, dass

11.3 - das Endgerät zweite Berechnungsmittel umfasst zum Berechnen (217) eines zweiten Verschlüsselungsschlüssels unter Verwendung des mindestens einen ersten Verschlüsselungsschlüssels, und

11.4 - das Endgerät Verschlüsselungsmittel umfasst zum Verschlüsseln/Entschlüsseln (311) der Daten, die zwischen dem Endgerät und dem Zugangspunkt übertragen werden, unter Verwendung des zweiten Verschlüsselungsschlüssels.

Darüber hinaus wird die Aufgabe auch durch die schriftsätzlich eingereichten Ansprüche der Hilfsanträge 1 bis 4 gelöst. Wegen der in der mündlichen Verhandlung zusätzlich gestellten Hilfsanträge wird auf die Ausführungen unter III. verwiesen.

Die geänderten Ansprüche 11 der Hilfsanträge 1 bis 4 lauten mit einer entsprechenden Merkmalsgliederung versehen, auf Deutsch folgendermaßen:

Hilfsantrag 1 (Änderungen zum Hauptantrag sind unter- bzw. durchgestrichen):

11 Drahtloses Endgerät, umfassend

11.1 einen Sende-Empfänger zum Aufbauen einer drahtlosen Verbindung mit einem Zugangspunkt in einem drahtlosen, lokalen Netzwerk und

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,
dadurch gekennzeichnet, dass

11.3 - das Endgerät zweite Berechnungsmittel umfasst zum Berechnen (217) eines zweiten Verschlüsselungsschlüssels unter Verwendung des ~~mindestens~~ mehr als einen ersten Verschlüsselungsschlüssels, und

11.4 - das Endgerät Verschlüsselungsmittel umfasst zum Verschlüsseln/Entschlüsseln (311) der Daten, die zwischen dem Endgerät und dem Zugangspunkt übertragen werden, unter Verwendung des zweiten Verschlüsselungsschlüssels.

Hilfsantrag 2 (Änderungen zum Hauptantrag sind unterstrichen):

11 Drahtloses Endgerät, umfassend

11.1 einen Sende-Empfänger zum Aufbauen einer drahtlosen Verbindung mit einem Zugangspunkt in einem drahtlosen, lokalen Netzwerk, wobei das Netzwerk kein DECT-Netzwerk ist, und

11.2 ein Identitätsmodul zum Berechnen (213) von mindestens einem ersten Verschlüsselungsschlüssel gemäß ~~dem~~ einem öffentlichen landgestützten Mobilnetz unter Verwendung eines Geheimschlüssels, welcher in dem Identitätsmodul gespeichert ist, und mindestens einem Challenge-Code, welcher von dem Mobilnetzwerk gesendet wird,

dadurch gekennzeichnet, dass

11.3 - das Endgerät zweite Berechnungsmittel umfasst zum Berechnen (217) eines zweiten Verschlüsselungsschlüssels unter Verwendung des mindestens einen ersten Verschlüsselungsschlüssels, und

11.4 - das Endgerät Verschlüsselungsmittel umfasst zum Verschlüsseln/Entschlüsseln (311) der Daten, die zwischen dem Endgerät und dem Zugangspunkt übertragen werden, unter Verwendung des zweiten Verschlüsselungsschlüssels.

Hilfsantrag 3 (Änderungen zum Hilfsantrag 1 sind unterstrichen):

11 Drahtloses Endgerät, umfassend

11.1 einen Sende-Empfänger zum Aufbauen einer drahtlosen Verbindung mit einem Zugangspunkt in einem drahtlosen, lokalen Netzwerk, wobei auf der MAC-Schicht ein Verfahren für Mehrfachzugriff mit Trägerprüfung und Kollisionsvermeidung, CSMA/CA, verwendet wird, und

11.2 ein Identitätsmodul zum Berechnen (213) von mehr als einem ersten Verschlüsselungsschlüssel gemäß einem öffentlichen landgestützten Mobilnetz unter Verwendung eines Geheimschlüssels, welcher in dem Identitätsmodul gespeichert ist, und mehr als einem Challenge-Code, welcher von dem Mobilnetzwerk gesendet wird,

dadurch gekennzeichnet, dass

11.3 - das Endgerät zweite Berechnungsmittel umfasst zum Berechnen (217) eines zweiten Verschlüsselungsschlüssels unter Verwendung des mehr als einen ersten Verschlüsselungsschlüssels, und

11.4 - das Endgerät Verschlüsselungsmittel umfasst zum Verschlüsseln/Entschlüsseln (311) der Daten, die zwischen dem Endgerät und dem Zugangspunkt übertragen werden, unter Verwendung des zweiten Verschlüsselungsschlüssels.

Hilfsantrag 4 (Änderungen zum Hilfsantrag 1 sind unterstrichen):

11 Drahtloses Endgerät, umfassend

11.1 einen Sende-Empfänger zum Aufbauen einer drahtlosen Verbindung mit einem Zugangspunkt in einem drahtlosen, lokalen Netzwerk gemäß IEEE802.11 Standard und

11.2 ein Identitätsmodul zum Berechnen (213) von mehr als einem ersten Verschlüsselungsschlüssel gemäß einem öffentlichen landgestützten Mobilnetz unter Verwendung eines Geheimschlüssels, welcher in dem Identitätsmodul gespeichert ist, und mehr als einem Challenge-Code, welcher von dem Mobilnetzwerk gesendet wird,

dadurch gekennzeichnet, dass

11.3 - das Endgerät zweite Berechnungsmittel umfasst zum Berechnen (217) eines zweiten Verschlüsselungsschlüssels unter Verwendung des mehr als einen ersten Verschlüsselungsschlüssels, und

11.4 - das Endgerät Verschlüsselungsmittel umfasst zum Verschlüsseln/Entschlüsseln (311) der Daten, die zwischen dem Endgerät und dem Zugangspunkt übertragen werden, unter Verwendung des zweiten Verschlüsselungsschlüssels.

Das beanspruchte drahtlose Endgerät umfasst demnach

- einen Sende-Empfänger,
- ein Identitätsmodul,
- zweite Berechnungsmittel und
- Verschlüsselungsmittel.

Zusätzlich müssen diese Bestandteile des Endgeräts so ausgelegt sein, dass sie die Eignungen entsprechend obigen Merkmalen haben, denn Zweckangaben definieren in einem Sachanspruch den durch das Patent geschützten Gegenstand, ohne diesen einzuschränken, regelmäßig dahin, dass er nicht nur die räumlich-körperlichen Merkmale erfüllen, sondern auch so ausgebildet sein muss, um für den im Patentanspruch angegebenen Zweck verwendbar zu sein (BGH, Urteil vom 19. Dezember 2017 – X ZR 5/16 –, juris Rn. 20). Dies bedeutet vorliegend, dass obige Komponenten des drahtlosen Endgeräts so ausgelegt sein müssen, dass sie die drahtlose Verbindung sowie das Berechnen der Verschlüsselungsschlüssel und das Verschlüsseln/Entschlüsseln der zwischen dem Endgerät und dem Zugangspunkt übertragenen Daten entsprechend den Angaben in den jeweiligen Ansprüchen 11 durchführen können.

Die Bedeutung der einzelnen Merkmale ergibt sich aus dem Streitpatent folgendermaßen:

Gemäß Abs. [0015] des Streitpatents ist das allgemein als „mobile terminal MT“ bezeichnete drahtlose Endgerät bspw. ein tragbarer Computer mit einer WLAN-Karte, einem SIM-Identitätsmodul *(Subscriber Identity Module)* und einer GSM-Mobilfunk-Komponente, wobei mittels eines Transceivers TxRx als Sende-Empfänger eine drahtlose Verbindung mit einem „access point AP“ als Zugangspunkt eines drahtlosen, lokalen Netzwerks aufgebaut werden kann.

Wie zudem in den Abs. [0012] bis [0014] erläutert wird, ist das drahtlose, lokale Netzwerk bspw. ein WLAN nach IEEE802.11 Standard und das öffentliche landgestützte Mobilnetz bspw. das GSM- und UMTS-Netz.

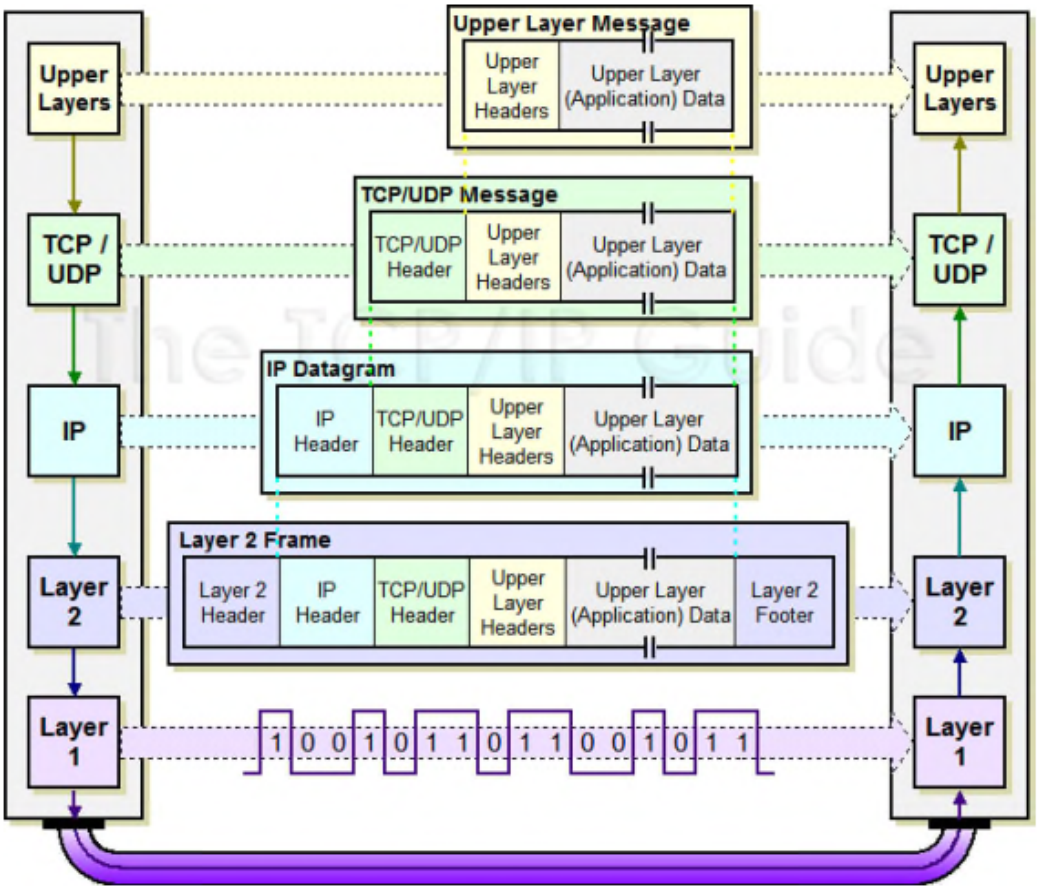
Entscheidend für die streitpatentgemäße Lehre ist die Berechnung des zweiten Verschlüsselungsschlüssels, unter dessen Verwendung die Daten zwischen dem Endgerät (MT) und dem Zugangspunkt (AP) verschlüsselt übertragen werden.

Dazu wird zunächst ein erster Verschlüsselungsschlüssel Kc berechnet, wobei zu dessen Berechnung gemäß Abs. [0014] auf der SIM-Karte der zur Kennung IMSI *(International Mobile Subscriber Identity)* des Endgeräts gehörende Geheimschlüssel *(secret key Ki)* und der Verschlüsselungsalgorithmus A8 (sozusagen als erstes Berechnungsmittel) gespeichert sind. Auch dem öffentlichen landgestützten Mobilnetz sind der Algorithmus A8 und der zur Kennung des Endgeräts gehörende Geheimschlüssel Ki bekannt (vgl. Abs. [0019], [0022] und [0024]). Im Mobilnetz wird auf Basis des Algorithmus A8, des Geheimschlüssels Ki und des einer Zufallszahl entsprechenden Challenge-Codes RAND der erste Verschlüsselungsschlüssel Kc berechnet (vgl. Abs. [0024]). Zusätzlich wird der Challenge-Code RAND vom Mobilnetz an das Endgerät gesendet, das dann ebenfalls auf Basis des Algorithmus A8, des Geheimschlüssels Ki und des Challenge-Codes RAND den ersten Verschlüsselungsschlüssel Kc berechnet. Somit verfügen dann sowohl das Endgerät als auch das Mobilnetz über den ersten Verschlüsselungsschlüssel Kc, ohne dass dieser gesendet werden muss.

Wie in Abs. [0028] erläutert, wird im Endgerät mit Hilfe zweiter Berechnungsmittel unter Verwendung des ersten Verschlüsselungsschlüssels Kc ein zweiter Verschlüsselungsschlüssel K berechnet. Unter Verwendung dieses zweiten Verschlüsselungsschlüssels werden mit Hilfe der im Endgerät vorhandenen Verschlüsselungsmittel die Daten, die zwischen dem Endgerät und dem Zugangspunkt übertragen werden, ver- und entschlüsselt.

Die Hilfsanträge beziehen sich insbesondere darauf, dass die zweiten Berechnungsmittel zum Berechnen eines zweiten Verschlüsselungsschlüssels unter Verwendung von mehr als einem ersten Verschlüsselungsschlüssel geeignet sind und das drahtlose, lokale Netzwerk kein DECT-Netzwerk, sondern gemäß IEEE802.11 gebildet ist bzw. auf der MAC-Schicht ein Verfahren für Mehrfachzugriff mit Trägerprüfung und Kollisionsvermeidung, CSMA/CA, verwendet wird.

Mit Eingabe vom 23. Januar 2019 und in der mündlichen Verhandlung am 24. Januar 2019 hat die Patentinhaberin das Merkmal 11.4 der jeweiligen Ansprüche 1, wonach das Endgerät Verschlüsselungsmittel umfasst zum Verschlüsseln/Entschlüsseln der Daten, die zwischen dem Endgerät und dem Zugangspunkt übertragen werden, dahingehend ausgelegt, dass aufgrund der Formulierung „der Daten“ in obigem Merkmal alle über das WLAN übertragenen Daten verschlüsselt würden, wobei unter dem Begriff „Daten“ alle Nutzdaten, d. h. die WLAN Payload zu verstehen seien. Es sei somit nicht anspruchsgemäß, wenn mit den Verschlüsselungsmittel nur manche der über das WLAN übertragenen Daten verschlüsselt würden, während andere Daten zwar verschlüsselt werden könnten, tatsächlich aber unverschlüsselt übertragen würden. Eine solch enge Auslegung des Merkmals 11.4 sei auch aufgrund der Beschreibung in den Absätzen [0002] und [0039] des Streitpatents geboten, denn demnach sei die Verbindung zwischen dem Endgerät und dem Zugangspunkt eine Verbindung auf der Schicht 2 des OSI-Schichtenmodells, vgl. „Layer 2“ der Anlage NB4.



Eine streitpatentgemäße Datenverschlüsselung müsse daher ebenfalls auf der zweiten OSI-Schicht erfolgen, insbesondere der MAC-Teilschicht von Schicht 2, und nur wenn der zweite Verschlüsselungsschlüssel auf der zweiten OSI-Schicht, bzw. der MAC Schicht zur Verschlüsselung eingesetzt würde, seien alle über die Verbindung zwischen dem Endgerät und dem Zugangspunkt übertragenen Nutzdaten, d. h. die gesamte WLAN Payload verschlüsselt, so dass maximale Vertraulichkeit gewährleistet sei. Dabei umfasse die Verschlüsselung der Daten auf der zweiten OSI-Schicht auch den IP-Header, aber nicht den Layer 2 Header, da dieser im Gegensatz zum IP-Header keine WLAN-Payload sei und dies die sinnvolle funktionelle Auslegung der beanspruchten Datenverschlüsselung sei.

Der Patentinhaberin ist zwar darin zuzustimmen, dass eine solche Datenverschlüsselung ein Verschlüsseln/Entschlüsseln der Daten, die zwischen dem Endgerät und dem Zugangspunkt übertragen werden, darstellt. Jedoch ist die streitpatentgemäße Lehre nicht darauf beschränkt.

Denn wie die Patentinhaberin auch in der mündlichen Verhandlung ausgeführt hat, werden bei einer Verschlüsselung auf der zweiten OSI-Schicht (Layer 2) nicht alle Daten eines Frames verschlüsselt, da der Layer 2 Header und der Layer 2 Footer unverschlüsselt bleiben, vgl. obige Anlage NB4. Der Fachmann legt das Merkmal 11.4 deshalb so aus, dass gerade nicht alle übertragenen Daten verschlüsselt werden müssen, sondern dass es in Übereinstimmung mit dem Ausführungsbeispiel von Abs. [0039] genügt, wenn die Daten eines Frames bzw. eines Informationspakets nur teilweise verschlüsselt werden, da dies auch bei dem beanspruchten Ausführungsbeispiel der Fall ist.

Der engen Auslegung der Patentinhaberin, wonach gemäß Merkmal 11.4 einerseits alle übertragenen Daten verschlüsselt würden, andererseits aber nur bestimmte Nutzdaten, d. h. Framedaten ohne Header und Footer, als die Daten im Sinne des Streitpatents anzusehen seien, die Daten des Headers und Footers eines Frames hingegen nicht, konnte sich der Senat daher nicht anschließen. Zudem hebt das Streitpatent in Abs. [0012] die allgemeine Anwendbarkeit der streitpatentgemäßen Lehre bei beliebigen drahtlosen, lokalen Netzwerken und öffentlichen landgestützten Mobilnetzen hervor, wohingegen das obige Ausführungsbeispiel auf dem IEEE802.11 WLAN-Standard basiert (vgl. Abs. [0036]: „in accordance with IEEE802.11“), während das beanspruchte Endgerät diesbezüglich nicht beschränkt ist.

Das Merkmal 11.4 der Ansprüche 1 ist deshalb insofern breit auszulegen, als das Verschlüsseln/Entschlüsseln der Daten sowohl alle als auch lediglich einen Teil der zwischen dem Endgerät und dem Zugangspunkt übertragenen Daten umfassen kann, jedoch zumindest die eigentlich zu übertragenden Nutzerdaten (Upper Layer (Application) Data in NB4), die als „die Daten“ im Minimum zu identifizieren sind, umfasst.

II.

Die drahtlosen Endgeräte der unabhängigen Ansprüche 11 nach Hauptantrag und nach den Hilfsanträgen 1 bis 4 sind nicht patentfähig, da sie zum Prioritätszeitpunkt des Streitpatents durch den vorgelegten Stand der Technik neuheitsschädlich vorweggenommen oder nahegelegt sind (Art. II § 6 Abs. 1 Nr. 1 IntPatÜG, Art. 138 Abs. 1 lit. a) EPÜ i. V. m. Art. 54 Abs. 1 bis 3und Art. 56 EPÜ).

Vor diesem Hintergrund kann neben der Zulässigkeit der Anspruchssätze auch dahinstehen, ob das Streitpatent in den verteidigten Fassungen eine ausführbare, technische und klare Lehre gibt.

Insbesondere kann dahingestellt bleiben, ob die Aufnahme des Disclaimers in Hilfsantrag 2 im Sinne eines negativ formulierten technischen Merkmals (hier: kein DECT-Netzwerk) zulässig ist, obwohl sich die dadurch bewirkte Beschränkung als technisch relevant erweist (BGH, Beschluss vom 25. Juli 2017 – X ZB 5/16 – Leitsatz b), Rn. 26).

1. Das drahtlose Endgerät gemäß dem erteilten Anspruch 11 nach Hauptantrag ist nicht patentfähig, weil es bezüglich der nachveröffentlichten älteren Anmeldung NK17, die die Priorität der Voranmeldung NiK-5prio beansprucht, nicht neu ist.

Die nur unter dem Aspekt der Neuheit relevante ältere Anmeldung NK17 (bzw. NiK-5), bei der zusätzlich der ggf. abweichende Offenbarungsgehalt der prioritätsbegründenden Voranmeldung (NiK-5prio) zu berücksichtigen ist, befasst sich mit der Authentisierung eines mobilen Knotens bzw. Terminals (MN bzw. MT) in einem Paketdatennetzwerk, insbesondere einem mobilen IP-Netzwerk (MIP, mobiles Internet-Protokoll), bei dem das mobile Terminal auch im fremden Netzwerk unter seiner heimischen IP-Adresse erreichbar sein soll.

Die Problemstellung, von der Druckschrift NK17 ausgeht, findet sich im zweiten Abs. von Beschreibungsseite 2 (inhaltlich übereinstimmend mit Seite 2, zweiter Abs. der Nik5-prio). Demnach wäre es wünschenswert, wenn das mobile Terminal authentisiert würde, sobald es eine Verbindung mit dem IP-Netzwerk herstellt. Eine Möglichkeit bestünde darin, dass sowohl das mobile Terminal als auch das IP-Netzwerk über ein beiden bekanntes und als Verschlüsselungsschlüssel eingesetztes gemeinsames Geheimnis verfügten (shared secret (is) to be used as the cryptographic key). Dazu müsste aber der Schlüssel auf sichere Weise in dem mobilen Terminal abgespeichert werden können. Andererseits sollte der Schlüssel hinsichtlich der Abhörsicherheit auch nicht einfach über das Netzwerk gesendet werden. Zudem sei davon auszugehen, dass sich das mobile Terminal mit einer Vielzahl von IP-Netzwerken verbinden werde und dann müsste das mobile Terminal über eine Datenbank mit einer Vielzahl von Geheimschlüsseln (secret keys) verfügen.

Ausgehend von dieser Problematik schlägt NK17 gemäß Seite 14, dritter Abs. (bzw. in NiK-5prio Seite 5, letzter Abs. und Seite 6, erster Abs.) vor, die Authentisierung unter Zuhilfenahme des im Mobilfunk verwendeten gemeinsamen Geheimnisses und des Subscriber Identity Moduls im mobilen Terminal durchzuführen.

Dementsprechend nennt Druckschrift NK17 als Beispiel für ein solches mobiles Terminal einen Laptop-Computer, der über einen WLAN-Adapter zur Verbindung mit einem drahtlosen, lokalen Netzwerk (wireless local area network) und über einen SIM-Karten-Leser mit SIM-Karte zur Verbindung mit einem öffentlichen, landgestützten Mobilnetz (GMS, UMTS) verfügt. Der Laptop kann sich mittels des WLAN-Adapters mit dem drahtlosen lokalen Netzwerk MIP, das über den „GSM Authentication Gateway GAGW“ an das GSM-Mobilnetz und die GSM-Kundendatenbank (Home Authentication, Authorisation and Accounting server HAAA) angeschlossen ist, verbinden, wobei der Laptop mittels der SIM-Karte authentisiert wird und über ein Mobilfunkadapter (RF2) auch direkt mit dem GSM- bzw. Mobilfunknetz verbunden sein kann, vgl. folgende Fundstellen in NK17 bzw. dem Prioritätsdokument (NiK-5prio):

- NK17, S. 1, Zn. 3 bis 11 und gleichlautend in NiK-5prio, S. 1, Zn. 5 bis 13: „[…] In mobile IP networking, a terminal, such as a laptop computer having a Wireless Local Area Network (WLAN) adapter coupled thereto, connects to its home agent via a foreign agent. […]“,
- Fig. 1 der NK17 bzw. NiK-5prio (aus dem Schriftsatz der Beklagten vom 11. September 2017):

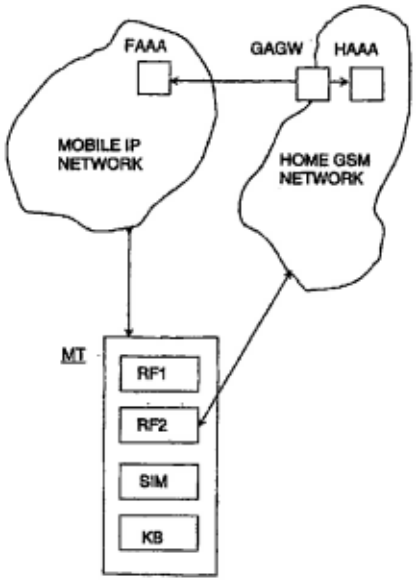


Fig. 1

Prioritätsdokument FI 20000760

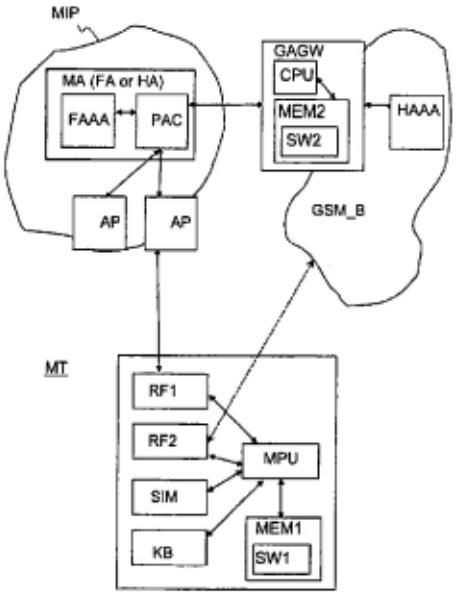


Fig. 1

Nachanmeldung WO‘134

- Beschreibung der Fig. 1 in NK17, S. 18, Z. 12 bis S. 19, Z. 26 bzw. entsprechend in NiK-5prio, S. 8, Zn. 7 bis 19 u. S. 9, Zn. 10 bis 25, wobei die im Prioritätsdokument fehlenden Teile zu streichen sind:
  “[…] The mobile node MT is typically a laptop computer with a wireless network adapter and software for networking. A plurality of mobile nodes MT can be attached to the MIP. […] Authentication is carried out using GSM-B and its SIM, SIM-B. […] The SIM-B is accessed by providing the MT (for example a laptop computer with a wireless local area network adapter) with a SIM card reader. […] Authentication can be further improved by using multiple RANDs in order to generate an authentication key which is more secure than just one Kc. […]”.

Aus obigen Fundstellen folgt somit, dass sich der Laptop mittels des Wireless Local Area Network (WLAN) – Adapters mit dem „fremden Agenten“ (FA bzw. FAAA) des mobilen IP-Netzwerks verbindet, der wiederum eine Verbindung zum „heimischen Agenten“ (HA bzw. HAAA) des GSM-Mobilnetzwerks herstellt. Somit umfasst in Übereinstimmung mit der Lehre des Streitpatents das mobile IP-Netzwerk (MIP) ein drahtloses lokales Netzwerk und das heimische GMS-Netzwerk ein öffentliches landgestütztes Mobilnetz.

Der obige die Authentisierung betreffende Abs. der NK17 bezieht sich u. a. auf die übliche Authentisierung in einem GSM-Netzwerk, die in der NK17, S. 17, Z. 16 bis S. 18, Z. 8 (entsprechend in NiK-5prio, S. 8, Z. 21 bis S. 9, Z. 8) folgendermaßen beschrieben ist:

> Operation of the SIM card in the GSM telecommunications network will now be explained. In GSM, there are known authentication algorithms which are referred to as A3 and A8. These algorithms run on the SIM and in the GSM telecommunications network. These algorithms and a GSM shared secret Ki are known by the SIM and the GSM telecommunications network operator, which typically stores them in an HLR (Home Location Register) of a Mobile services Switching Centre (MSC).
>
> In authentication, the GSM telecommunications network operator generates a challenge RAND that is a 128 bit random code, which is to be used as a challenge, a corresponding 64 bit GSM session key Kc and a 32 bit signed response SRES for verifying the response to the challenge. The 64 bit session GSM session key Kc is generated by the A8 algorithm as A8 (Ki, RAND) and the 32 bit long SRES is generated by the A3 (Ki, RAND). The combination RAND, SRES and Kc is generally referred to as a GSM triplet. The GSM telecommunications network operator sends the RAND to its subscriber (GSM telephone), the RAND is received by the subscriber and the subscriber passes it to the SIM, which reproduces SRES and Kc. Then the SIM responds to the challenge by sending the SRES. The operator receives the SRES and can confirm the identity of the SIM. The GSM telecommunications network operator can also verify that it shares a Kc with the SIM.

> **Then the Kc can then be used to encrypt data traffic over a GSM radio channel**. The advantage of this challenge- response mechanism is that Kc never need be sent over the GSM radio channel and thus it cannot be eavesdropped.

Demnach ist in dem SIM-Identitätsmodul des Laptops neben den A3- und A8-Algorithmen ein individueller Geheimschlüssel (GSM shared secret Ki) gespeichert, wobei diese Algorithmen und der Geheimschlüssel Ki auch dem GSM-Netzwerk insbesondere durch das HLR-Register bekannt sind. Im Rahmen der Authentisierung generiert das GSM-Netzwerk einen Challenge-Code (challenge RAND), den es an das SIM-Identitätsmodul sendet. Dieses berechnet daraus die Bestätigungsantwort SRES und den GSM-Session Key Kc, mit dem die GSM-Daten verschlüsselt werden („[…] the Kc can then be used to encrypt data traffic […].“).

Da der Begriff „session key“ ein dem Fachmann bekannter einschlägiger Fachbegriff ist, mit dem ein Schlüssel (key) bezeichnet wird, der für eine bestimmte Sitzung (session) gültig ist und der Ver- und Entschlüsselung der übertragenen Daten dient, bestätigen sowohl die obige Fundstelle als auch die Erläuterungen im Zusammenhang mit der grundsätzlichen Aufgabenstellung auf Seite 2, zweiter Abs., wonach das gemeinsame Geheimnis bzw. der Session Key dem Verschlüsseln der Daten dient („shared secret is to be used as the cryptographic key“,) das fachmännische Verständnis der Begriffe „Session Key“ und „Shared Secret“ als einen Verschlüsselungsschlüssel.

Der ein SIM- und GSM-Modul aufweisende Laptop weist folglich auch Ver- und Entschlüsselungsmittel zum Ver- und Entschlüsseln von Daten auf.

Zudem weist Druckschrift NK17 in obigen Fundstellen darauf hin, dass die Authentisierung durch die Verwendung mehrerer RANDs zur Berechnung von Kc-Werten verbessert werden kann.

Die Authentisierung in dem kombinierten Netzwerk entsprechend Fig. 1 wird in NK17, S. 19, Z. 28 bis S. 21, Z. 3 bzw. in NiK-5prio, S. 9, Z. 27 bis S. 11 anhand von zehn Authentisierungsschritten beschrieben, von denen hinsichtlich des beanspruchten mobilen Endgeräts insbesondere die Schritte 3 bis 10 relevant sind.

So berechnet das GSM-Netzwerk in Schritt 3 des Authentisierungsprozesses ähnlich wie in der GSM-Authentisierung einen oder mehrere Challenge-Codes (n Rands) und aus dem Geheimschlüssel Ki einen oder mehrere erste Verschlüsselungsschlüssel Kc. Zusätzlich wird unter Verwendung von einem oder mehreren der ersten Verschlüsselungsschlüssel Kc der gemeinsame Session Key K (shared session key, vgl. NK17, S. 19, Z. 15 bzw. NiK-5prio, S. 9, Z. 12) berechnet.

Gemäß den Schritten 4 bis 7 werden dann ein oder mehrere Challenge-Codes (n Rands) vom GSM-Netzwerk zum SIM-Identitätsmodul des Endgeräts bzw. Laptops gesendet, wo der oder die ersten Verschlüsselungsschlüssel Kc sowie der gemeinsame Session Key K in entsprechender Weise ebenfalls berechnet werden. Damit verfügen das Endgerät (MT), das lokale Netzwerk (FAAA) und das Mobilnetz (HAAA) über einen gemeinsamen Session Key K, vgl. in obiger Fundstelle der NiK-5prio den Schritt 10: „Authentication is complete and the FAAA and the terminal share the session key K“.

Dass die übertragenen Daten unter Verwendung des gemeinsamen Session Keys K verschlüsselt werden, ergibt sich, wie bereits dargelegt, für den Fachmann

- aus dem einschlägigen Begriff „session key“, der einen Verschlüsselungsschlüssel bezeichnet,
- aus der Bezugnahme auf den normalen GSM-Authentisierungsprozess in NK17 auf S. 17, Z. 26 u. S. 18, Zn. 5 und 6, wonach der Session Key der Verschlüsselung der übertragenen Daten dient,

- und auch aus der allgemeinen Beschreibung auf Seite 2, zweiter Abs., wonach der gemeinsame Geheimschlüssel bzw. das gemeinsame Geheimnis als Verschlüsselungsschlüssel eingesetzt wird.

Hauptantrag

Damit offenbart die ältere Anmeldung NK17 unter Berücksichtigung der Offenbarung im prioritätsbegründenden Dokument NiK-5prio mit den Worten des erteilten Anspruchs 11 gemäß Hauptantrag ein

11 Drahtloses Endgerät *(laptop computer having a Wireless Local Area Network (WLAN) adapter coupled thereto / vgl. S. 1, Zn. 7 u. 8 sowie S. 19, Zn. 20 u. 21:* „*The SIM-B is accessed by providing the MT (for example a laptop computer with a wireless local area network adapter) with a SIM card reader.")*, umfassend

11.1 einen Sende-Empfänger *(Wireless Local Area Network (WLAN) adapter / vgl. obige Fundstellen)* zum Aufbauen einer drahtlosen Verbindung mit einem Zugangspunkt in einem drahtlosen, lokalen Netzwerk und

11.2 ein Identitätsmodul *(Subscriber Identity Module (SIM) / vgl. S. 15, Zn. 31, 32 sowie SIM card reader / vgl. obige Erläuterungen u. Fundstellen)* zum Berechnen von mindestens einem ersten Verschlüsselungsschlüssel *(Kc vgl. obige Erläuterungen u. Fundstellen)* gemäß einem öffentlichen landgestützten Mobilnetz *(GSM network / vgl. obige Erläuterungen u. Fundstellen)* unter Verwendung eines Geheimschlüssels (Ki / *vgl. obige Erläuterungen u. Fundstellen)*, welcher in dem Identitätsmodul *(SIM)* gespeichert ist,

und mindestens einem Challenge-Code *(n RANDs / vgl. S. 20, Zn. 6 bis 28)*, welcher von dem Mobilnetzwerk gesendet wird,

wobei

11.3 - das Endgerät *(laptop computer)* zweite Berechnungsmittel umfasst zum Berechnen eines zweiten Verschlüsselungsschlüssels *(shared session Key K / vgl. S. 19, Z. 15 u. S. 20, Zn. 6 bis 28)* unter Verwendung des mindestens einen ersten Verschlüsselungsschlüssels *(Kc / vgl. S. 20, Zn. 6 bis 28)*, und

11.4 - das Endgerät *(laptop computer)* Verschlüsselungsmittel umfasst zum Verschlüsseln/Entschlüsseln der Daten, die zwischen dem Endgerät und dem Zugangspunkt übertragen werden *(vgl. analog S. 17, Z. 26 u. S. 18, Zn. 5 und 6)*, unter Verwendung des zweiten Verschlüsselungsschlüssels *(shared session Key K)*.

Die ältere Anmeldung NK17 offenbart daher auch unter Berücksichtigung des Offenbarungsgehalts der prioritätsbegründenden Anmeldung NiK-5prio ein drahtloses Endgerät mit sämtlichen Merkmalen des erteilten Anspruchs 11 nach Hauptantrag, das daher wegen fehlender Neuheit nicht patentfähig ist.

Hilfsantrag 1

Das Zusatzmerkmal des Anspruchs 11 nach Hilfsantrag 1, wonach mehrere erste Verschlüsselungsschlüssel, d. h. mehrere Kcs, unter Verwendung des in dem Identitätsmodul gespeicherten Geheimschlüssels (Ki) und mehrere Challenge-Codes (n RANDs) berechnet werden, und wonach der zweite Verschlüsselungsschlüssel (K) unter Verwendung von mehreren ersten Verschlüsselungsschlüsseln (Kc) berechnet wird, ist ebenfalls aus der älteren Anmeldung NK17 bekannt, vgl. deren Ansprüche 11 u. 12 (bzw. 9 bis 11 der NiK-5prio) sowie S. 20, Zn. 6 bis 28 der Beschreibung (bzw. S. 10 der NiK-5prio).

Denn dort ist angegeben, dass zum einen mehrere Kcs unter Verwendung mehrerer RANDs berechnet werden und dass zum anderen der zweite Verschlüsselungsschlüssel (session key K) unter Verwendung mehrerer erster Verschlüsselungsschlüssel (n*Kc) berechnet wird.

Wie zudem auf S. 19, Zn. 24 bis 26 der NK17 (bzw. S. 9, Zn. 23 bis 25 der NiK-5prio) erläutert ist, dient dies der Erhöhung der Sicherheit.

Hilfsantrag 2

Das drahtlose Endgerät nach Anspruch 11 des Hilfsantrags 2 ist in Merkmal 11.1 dahingehend präzisiert, dass es

einen Sende-Empfänger umfasst zum Aufbauen einer drahtlosen Verbindung mit einem Zugangspunkt in einem drahtlosen, lokalen Netzwerk, wobei das Netzwerk kein DECT-Netzwerk ist.

Der Sende-Empfänger des beanspruchten drahtlosen Endgeräts muss demnach dazu geeignet sein, eine drahtlose Verbindung zu einem Zugangspunkt eines drahtlosen, lokalen Netzwerks aufzubauen, das kein DECT-Netzwerk ist.

Diese Eignung hat der WLAN-Adapter des Laptops aus Druckschrift NK17 bzw. NiK-5prio. Denn wie bspw. in Druckschrift NK20 unter Kap. III beschrieben ist, gab es zum Prioritätszeitpunkt in Europa zwei WLAN-Standards (IEEE 802.11, HIPERLAN), weshalb der in Druckschrift NK17 offenbarte WLAN-Adapter zumindest für eines dieser beiden Netzwerke geeignet sein muss. Da keines dieser beiden Netzwerke ein DECT-Netzwerk ist, entnimmt der Fachmann der Druckschrift NK17 unmittelbar und eindeutig das Zusatzmerkmal des Anspruchs 11 von Hilfsantrag 2.

Das drahtlose Endgerät nach Anspruch 11 des Hilfsantrags 2 ist somit wegen fehlender Neuheit bezüglich der älteren Anmeldung NK17 nicht patentfähig.

2. Druckschrift NK23, die ein „Internet Draft“ der IETF (Internet Engineering Task Force) ist und auf der ersten Seite das Datum „June 2000“ aufweist, stellt vorveröffentlichten Stand der Technik dar, denn das Dokument NK23a belegt die öffentliche Zugänglichkeit solcher „Internet Drafts“ und die Email vom 20. Juni 2000 gemäß Anlage NK23b, in der angezeigt wird, dass die Druckschrift NK23 vom 19. Juni 2000 online verfügbar ist, bestätigt, dass diese Druckschrift vor dem Prioritätstag (30. Juni 2000) des Streitpatents öffentlich verfügbar war.

Das Dokument NK23 befasst sich ebenfalls mit der Authentisierung in einem mobilen IP-Netzwerk (mobiles Internet-Protokoll, MIP), vgl. deren Titel mit Abstract. Da sich Druckschrift NK23 an den ausgewiesenen Fachmann richtet, ist der Aufbau eines solchen Netzwerks dort nur schematisch skizziert und lediglich angegeben, dass es einen mobilen Knoten (mobile node) mit einem SIM-Identitätsmodul, einen mobilen Agenten (mobility agent) und ein Mobilnetz in Gestalt des GSM-Netzwerks (GSM-network) umfasst, wobei der mobile Knoten über den mobilen Agenten mit dem GSM-Netzwerk in Verbindung steht, vgl. deren Kapitel 3.1 und 3.2 mit Fig. 1, insbesondere den letzten Abs. von Kap. 3.2 und Fig. 1.

Da somit die genaue Ausgestaltung des mobilen IP-Netzwerks dem Fachmann überlassen bleibt, wird dieser das IP-Netzwerk in üblicher Weise, wie bspw. in Druckschrift NK11 dargestellt, ausbilden.

Ähnlich wie Druckschrift NK23 skizziert auch Druckschrift NK11 ein mobiles IP-Netzwerk (MIP) zunächst in allgemeiner Form als aus mobilen Knoten (mobile node) und mobilen Agenten (home agent, foreign agent) bestehend, vgl. Seite 1, letzter Abs., um dann anhand von Fig. 1 die typische Ausgestaltung eines solchen Netzwerks zu erläutern, vgl. S. 3, Z. 31 bis S. 4, Z. 30.

Demnach ist der mobile Knoten ein Laptop mit einem SIM-Identitätsmodul (SIM) und einem Sende-Empfänger (wireless LAN interface) zum Aufbauen einer drahtlosen Verbindung mit einem Zugangspunkt (access point AP1) in einem drahtlosen, lokalen Netzwerk (local area network LAN1), vgl. Fig. 1 und S. 4, Zn. 3 bis 22.

Über das lokale Netzwerk ist der Laptop mit dem mobilen Agenten verbunden, d. h. über den fremden Agenten (foreign agent FA) mit dem heimischen Agenten (home agent), der wiederum an das GSM-Netzwerk gekoppelt ist *(vgl. S. 4, Zn. 23 bis 30: „The figure also shows the home agent HA of terminal TE1, which is located in connection with the router R3 connected to the Internet. In practice, the organisation owning the home agent often functions not only as an ISP (Internet Service Provider) operator but also as a mobile communications operator, for which reason it is possible from the home agent HA freely to establish a connection to the mobile communications network. In practice, the router, which has a home agent function, and the home location register may be located e.g. in the same equipment premises.“).*

Basierend auf einem solchen mobilen IP-Netzwerk wird in dem Dokument NK23 die Berechnung von Verschlüsselungsschlüsseln beschreiben.

Dazu verweist Druckschrift NK23 im ersten Abs. von Seite 3 zunächst auf die übliche GSM-Authentisierung, bei der das GSM-Netzwerk dem SIM-Identitätsmodul des Endgeräts einen Challenge-Code (random number RAND) zusendet, das daraus zusammen mit dem im SIM-Identitätsmodul gespeicherten Geheimschlüssel Ki einen ersten Verschlüsselungsschlüssel Kc berechnet, der im GSM-System auch zur Datenverschlüsselung eingesetzt wird (encryption key over the air interface).

Dies ist entsprechend im GSM-Standard hinterlegt, vgl. NK9c, Kap. 4, insbesondere Kap. 4.2 und 4.3, wo explizit beschrieben ist, dass der Schlüssel Kc im GSM-Netzwerk im Rahmen der Authentisierung der Verschlüsselung der übermittelten Daten dient, indem die Daten unter Verwendung des Verschlüsselungsschlüssels Kc (ciphering key Kc) und des A5-Algorithmus ver- und entschlüsselt werden. Der Fachmann weiß somit, dass diese im Rahmen der Authentisierung berechneten Verschlüsselungsschlüssel Kc zur Verschlüsselung verwendet werden.

Im anschließenden zweiten Abs. von Seite 3 der NK23 ist die im mobilen IP-Netzwerk zusätzlich erfolgende Berechnung eines zweiten Verschlüsselungsschlüssels folgendermaßen zusammengefasst: „In SIM key exchange, several RAND challenges are used for generating several 64-bit Kc keys, which are combined to constitute a longer Mobile IP authentication key."

Demnach werden im mobilen IP-Netzwerk aus mehreren Challenge-Codes mehrere erste Verschlüsselungsschlüssel Kc berechnet, die mittels einer Abbildungsvorschrift zu einem mobilen IP-Authentisierungsschlüssel (mobile IP authentication key) kombiniert werden, vgl. auch S. 3, dritter Abs. der NK23.

Der berechnete „mobile IP authentication key" ist gemäß dem vierten Abs. von Seite 3 der NK23 gleichzeitig der „shared session key". Wie bereits zur Druckschrift NK17 ausgeführt wurde, ist dies ein dem Fachmann bekannter einschlägiger Fachbegriff, mit dem ein den beiden am Datenaustausch beteiligten Einheiten bekannter Schlüssel (shared key) bezeichnet wird, der für eine bestimmte Sitzung (session) gültig ist und der Ver- und Entschlüsselung der übertragenen Daten dient. Somit ist der aus den mehreren ersten Verschlüsselungsschlüsseln Kc berechnete mobile IP-Authentisierungsschlüssel ein zweiter Verschlüsselungsschlüssel K, was, wie auch bei Druckschrift NK17, durch den Verweis auf den GSM-Verschlüsselungsschlüssel Kc unterstrichen wird, der entsprechend obigen Erläuterungen standardmäßig zur Verschlüsselung übertragener GSM-Daten verwendet wird.

Wie im Kap. 3.1 der NK23 auf S. 5, letzter Abs. beschrieben ist, erfolgt die Berechnung des als „key K" bezeichneten Mobile IP authentication key mittels einer speziellen Hash-Berechnungsvorschrift aus mehreren Kcs (n*Kc).

Hauptantrag

Damit ergibt sich das Endgerät des erteilten Anspruchs 11 gemäß Hauptantrag in naheliegender Weise aus Druckschrift NK23 i.V.m dem durch Druckschrift NK11 belegten Fachwissen betreffend den üblichen Aufbau eines mobilen IP-Netzwerks. Denn diesen Druckschriften entnimmt der Fachmann ein

11 Drahtloses Endgerät *(mobile node / vgl. NK23, S. 3, dritter Abs.; bzw. laptop / vgl. NK11, Fig. 1 u. S. 3, Z. 31 bis S. 4, Z. 30)*, umfassend

11.1 einen Sende-Empfänger *(LAN interface, wireless manner / vgl. NK11, Fig. 1 u. S. 4, Zn. 3 bis 6)* zum Aufbauen einer drahtlosen Verbindung mit einem Zugangspunkt *(access poin AP1 / vgl. NK11, Fig. 1)* in einem drahtlosen, lokalen Netzwerk *(local area network LAN1, wireless / vgl. NK11, Fig. 1 u. S. 4, Zn. 3 bis 6*) und

11.2 ein Identitätsmodul *(Subscriber Identity Module (SIM) / vgl. NK23, S. 2, vorletzter Abs.; bzw. NK11, Fig. 1 u. S. 4, Zn. 12 u. 13)* zum Berechnen von mindestens einem ersten Verschlüsselungsschlüssel *(Kc / vgl. NK23, S. 3, erster u. zweiter Abs.)* gemäß einem öffentlichen landgestützten Mobilnetz *(GSM network / vgl. NK23, S. 3, erster u. zweiter Abs. sowie S. 6, Kap. 3.2, letzter Abs.)* unter Verwendung eines Geheimschlüssels *(Ki / vgl. NK23, S. 3, erster Abs.)*, welcher in dem Identitätsmodul *(SIM)* gespeichert ist, und mindestens einem Challenge-Code *(several RAND challenges / vgl. NK23, S. 3, erster u. zweiter Abs.)*, welcher von dem Mobilnetzwerk (*GSM network*) gesendet wird,

wobei

11.3 - das Endgerät *(mobile node / vgl. NK23, S. 3, zweiter u. dritter Abs.)* zweite Berechnungsmittel umfasst zum Berechnen eines zweiten Verschlüsselungsschlüssels *(mobile IP authenication key K, shared session key K / vgl. NK23, S. 3, zweiter bis vierter Abs)*

unter Verwendung des mindestens einen ersten Verschlüsselungsschlüssels *(Kc / vgl. NK23, S. 3, zweiter u. dritter Abs.)* und

11.4 - das Endgerät *(mobile node)* Verschlüsselungsmittel *(bspw. im SIM-Identitätsmodul)* umfasst zum Verschlüsseln/Entschlüsseln der Daten, die zwischen dem Endgerät und dem Zugangspunkt übertragen werden *(vgl. NK23, S. 3, erster Abs u. obige Ausführungen)*, unter Verwendung des zweiten Verschlüsselungsschlüssels *(mobile IP authenication key K, shared session key K / vgl. NK23, S. 3, zweiter bis vierter Abs.)*.

Das Endgerät des erteilten Anspruchs 11 nach Hauptantrag wird dem Fachmann daher ausgehend von Druckschrift NK23 i. V. m. seinem durch Druckschrift NK11 belegten Fachwissen nahegelegt und ist wegen fehlender erfinderischer Tätigkeit nicht patentfähig.

Hilfsantrag 1

Das Zusatzmerkmal des Hilfsantrags 1, dass mehrere erste Verschlüsselungsschlüssel, d. h. mehrere Kcs, unter Verwendung des in dem Identitätsmodul gespeicherten Geheimschlüssels (Ki) und mehrerer Challenge-Codes (several RAND challenges) berechnet werden, und wonach der zweite Verschlüsselungsschlüssel (mobile IP authenication key K, shared session key K) unter Verwendung von mehreren ersten Verschlüsselungsschlüsseln (Kc) berechnet wird, ist ebenfalls aus der Druckschrift NK23 bekannt, vgl. deren Seite 3, erster u. zweiter Abs. sowie die Hash-Funktion h(n*Kc | nonceMN) zur Berechnung des Schlüssels K auf Seite 5, letzter Abs.

Das Endgerät nach Anspruch 11 von Hilfsantrag 1 wird dem Fachmann daher ausgehend von Druckschrift NK23 i. V. m. seinem durch Druckschrift NK11 belegten Fachwissen nahegelegt und ist wegen fehlender erfinderischer Tätigkeit nicht patentfähig.

Hilfsantrag 2

Die weitere Beschränkung in Merkmal 11.1 des Anspruchs 11 von Hilfsantrag 2, wonach das Netzwerk kein DECT-Netzwerk ist, entnimmt der Fachmann der Druckschrift NK11. Denn wie in Druckschrift NK20 unter Kap. III beschrieben ist, gab es zum Prioritätszeitpunkt in Europa zwei WLAN-Standards (IEEE 802.11, HIPERLAN), weshalb die in Druckschrift NK11 offenbarte WLAN-Schnittstelle zumindest für eines dieser beiden Netzwerke geeignet sein muss. Da keines dieser beiden Netzwerke ein DECT-Netzwerk ist, wird auch das Endgerät nach Anspruch 11 von Hilfsantrag 2 dem Fachmann ausgehend von Druckschrift NK23 i. V. m. seinem durch Druckschrift NK11 belegten Fachwissen nahegelegt, weshalb es wegen fehlender erfinderischer Tätigkeit nicht patentfähig ist.

Hilfsantrag 3

Auch die Beschränkung in Merkmal 11.1 des Anspruchs 11 von Hilfsantrag 3, wonach auf der MAC-Schicht ein Verfahren für Mehrfachzugriff mit Trägerprüfung und Kollisionsvermeidung, CSMA/CA, verwendet wird, ergibt sich für den Fachmann in naheliegender Weise aus Druckschrift NK11. Denn gemäß Druckschrift NK20, vgl. deren Kap. III und Fig. 7, gab es zum Prioritätszeitpunkt des Streitpatents in Europa zwei WLAN-Standards, nämlich IEEE 802.11 und HIPERLAN, von denen der – im Gegensatz zu HIPERLAN – damals kommerziell verfügbare IEEE 802.11-Standard das CSMA//CA-Verfahren verwendet, vgl. Fig. 7 der NK20. Da es für den Fachmann naheliegend ist, aus den beiden alternativen Standards (HIPERLAN, IEEE 802.11) den IEEE 802.11-Standard aufgrund dessen kommerziellen Verfügbarkeit auszuwählen, und dieser Standard das beanspruchte Mehrfachzugriffsverfahren verwendet, ergibt sich auch das Endgerät von Anspruch 11 nach Hilfsantrag 3 für den Fachmann in naheliegender Weise ausgehend von Druckschrift NK23 i. V. m. seinem durch Druckschrift NK11 belegten Fachwissen. Dieses ist daher wegen fehlender erfinderischer Tätigkeit nicht patentfähig.

Hilfsantrag 4

Anspruch 11 des Hilfsantrags 4 ist in Merkmal 11.1 dahingehend präzisiert, dass das drahtlose, lokale Netzwerk ein Netzwerk gemäß IEEE802.11 Standard ist.

Wie bereits zu Hilfsantrag 3 ausgeführt, war es zum Prioritätszeitpunkt für den Fachmann nahliegend, die in Druckschrift NK11 offenbarte WLAN-Schnittstelle als IEEE802.11-WLAN-Schnittstelle auszubilden, so dass Druckschrift NK23 dem Fachmann i. V. m. dessen durch Druckschrift NK11 belegten Fachwissen das Endgerät von Anspruch 11 nach Hilfsantrag 4 nahelegt. Dieses ist folglich wegen fehlender erfinderischer Tätigkeit nicht patentfähig.

3. Druckschrift NK9a ist ein Dokument zum DECT-Standard (Digital European Cordless Telecommunications bzw. Digital Enhanced Cordless Telecommunications), das sich mit der Einbindung des GSM- Mobilfunksystems in das üblicherweise bei tragbaren Festnetztelefonen eingesetzte DECT-System befasst, vgl. S. 7, Kap. 1, zweiter Abs. *„To enable DECT terminals to inter-work with DECT systems which are connected to the GSM infrastructure […]“*.

Ein solches DECT-System umfasst neben der Basisstation (DECT Fixed Part FP) tragbare drahtlose Endgeräte (DECT Portable Part PP), die zusätzlich mit einem SIM-Identitätsmodul zur Bereitstellung der GSM-Mobilfunk-Funktionalität ausgestattet sind (vgl. S. 7, vorletzter Abs.: *„The DECT PP has to accept the GSM Subscriber Identification Module (SIM) as well as the DECT Authentification Module (DAM), with a GSM application“*).

Gemäß den Definitionen der Basisstation (FP) und der drahtlosen Endgeräte (PP) in NK9a, S. 12 und 13 ist die Basisstation (FP) ein Zugangspunkt in einem drahtlosen, lokalen Netzwerk (vgl. obige Definitionen mit den Begriffen: local network, air interface, radio transmission elements), und der tragbare Teil (PP) ist ein drahtloses Endgerät mit einem Sende-Empfänger (radio transmission elements) zum Aufbauen einer drahtlosen Verbindung mit dem Zugangspunkt (FP) in dem drahtlosen, lokalen Netzwerk (local network, air interface).

Zudem nimmt NK9a auf S. 8 unter Punkt [2] ausdrücklich Bezug auf das weitere den DECT-Standard betreffende Dokument NK9b, in dem unter Kap. 5 auf S. 23 Anwendungsmöglichkeiten des DECT-Standards und insbesondere auch der Einsatz als drahtloses, lokales Netzwerk beschrieben werden (cordless data - Local Area Networks (LANs), local public network).

Somit ist aus Druckschrift NK9a i.V.m. NK9b ein drahtloses Endgerät mit den Merkmalen 11 und 11.1 des erteilten Anspruchs 1 nach Hauptantrag bekannt.

Wie bereits ausgeführt, weist das tragbare DECT-Endgerät eine SIM-Schnittstelle als Identitätsmodul auf, mit der die SIM- und GSM-Funktionalität bereitgestellt wird, vgl. auch Kap. 8.5 auf S. 23.

Zudem wird im Unterpunkt 8.3.1.10 auf Seite 20 hervorgehoben, dass die übertragenen Daten mit einem zweiten Verschlüsselungsschlüssel (DECT cipher key), der von dem GSM-Verschlüsselungsschlüssel Kc (GSM cipher key) als erstem Verschlüsselungsschlüssel abgeleitet wird, verschlüsselt werden können:

> 8.3.1.10 Support of DECT encryption
> The provision shall be made for support on the PP of no encryption, or support of encryption based on the DECT standard cipher. The DECT cipher key shall be derived from the GSM cipher key, Kc.

Somit muss das Endgerät Berechnungsmittel umfassen, mit denen es den DECT-Verschlüsselungsschlüssel vom GSM-Verschlüsselungsschlüssel ableitet.

Da der GSM Verschlüsselungsschlüssel zwangsläufig gemäß dem GSM-Standard NK9c berechnet werden muss, was mit einem weiteren Berechnungsmittel erfolgt, sind auch die Merkmale 11.2 bis 11.4 des erteilten Anspruchs 11 bei dem in Druckschrift NK9a beschriebenen DECT-Endgerät erfüllt, denn der GSM-Standard NK9c gibt auf S. 51 unter Punkt C.3.1 Folgendes vor:

As defined in TS GSM 03.20, Algorithm A8 must compute the ciphering key Kc from the random challenge RAND sent during the authentication procedure, using the authentication key Ki.

Folglich umfasst das in NK9a beschriebene drahtlose Endgerät *(Portable Part PP)* in Übereinstimmung mit dem erteilten Anspruch 11

11.1 einen Sende-Empfänger *(radio transmission elements)* zum Aufbauen einer drahtlosen Verbindung mit einem Zugangspunkt *(Fixed Part FP)* in einem drahtlosen, lokalen Netzwerk *(cordless data - Local Area Networks (LANs)* und

11.2 ein Identitätsmodul *(GSM Subscriber Identification Module (SIM))* zum Berechnen von mindestens einem ersten Verschlüsselungsschlüssel *(GSM cipher key Kc)* gemäß einem öffentlichen landgestützten Mobilnetz *(GSM)* unter Verwendung eines Geheimschlüssels *(Ki.)*, welcher in dem Identitätsmodul *(SIM)* gespeichert ist, und mindestens einem Challenge-Code *(random challenge RAND.)*, welcher von dem Mobilnetzwerk (*GSM*) gesendet wird,

wobei

11.3 - das Endgerät *(PP)* zweite Berechnungsmittel umfasst zum Berechnen eines zweiten Verschlüsselungsschlüssels *(DECT cipher key)* unter Verwendung des mindestens einen ersten Verschlüsselungsschlüssels *(Kc)* und

11.4 - das Endgerät *(Portable Part PP)* Verschlüsselungsmittel *(DECT encryption)* umfasst zum Verschlüsseln/Entschlüsseln der Daten, die zwischen dem Endgerät (PP) und dem Zugangspunkt (FP) übertragen werden, unter Verwendung des zweiten Verschlüsselungsschlüssels *(DECT cipher key)*.

Die Druckschrift NK9a offenbart daher zusammen mit den Druckschriften NK9b und NK9c, auf die in NK9a ausdrücklich Bezug genommen wird, ein drahtloses Endgerät mit sämtlichen Merkmalen des erteilten Anspruchs 11 nach Hauptantrag. Das drahtlose Endgerät nach Anspruch 11 des Hauptantrags ist daher wegen fehlender Neuheit bzgl. der Druckschrift NK9a, die explizit auf die Druckschriften 9b und 9c Bezug nimmt, nicht patentfähig.

III.

Die in der mündlichen Verhandlung am 24. Januar 2019 eingereichten Hilfsanträge 0a und 0b sind nach § 83 Abs. 4 Satz 1 PatG als verspätet zurückzuweisen, genau wie die ebenfalls hilfsweise beantragten Fassungen a und b der Hilfsanträge 1 bis 4.

Damit ist über die Verteidigung des Streitpatents nach diesen Hilfsanträgen in der Sache nicht zu entscheiden.

1. Gemäß § 83 Abs. 4 Satz 1 PatG kann das Patentgericht eine Verteidigung des Beklagten mit einer geänderten Fassung des Patents zurückweisen und bei seiner Entscheidung unberücksichtigt lassen, wenn dieses Vorbringen nach Ablauf der hierfür nach § 83 Abs. 2 PatG gesetzten Frist erfolgt ist und die weiteren Voraussetzungen des § 83 Abs. 4 Satz 1 Nrn. 1 bis 3 PatG erfüllt sind.

a) Mit qualifiziertem Hinweis vom 12. September 2018, der der Beklagten am 17. September 2018 zugestellt worden ist, wurde eine Frist zur beiderseitigen Äußerung und abschließenden Stellungnahme bis zum 15. November 2018 gesetzt.

Die Verteidigung des Streitpatents nach den Hilfsanträgen 0a und 0b sowie mit den entsprechend abgewandelten Fassungen der Hilfsanträge 1 bis 4 ist erst in der mündlichen Verhandlung vom 24. Januar 2019 um 13:25 Uhr erfolgt und damit erst nach der nach § 83 Abs. 2 PatG gesetzten Frist.

b) Eine Berücksichtigung dieser Hilfsanträge hätte eine Vertagung der bereits begonnenen mündlichen Verhandlung erforderlich gemacht (§ 83 Abs. 4 Satz 1 Nr. 1 PatG).

Die Berücksichtigung der Hilfsanträge hätte eine Vertagung der mündlichen Verhandlung nach § 99 Abs. 1 PatG i. V. m. § 227 Abs. 1 ZPO insoweit erforderlich gemacht, als den Klägerinnen hätte Gelegenheit gegeben werden müssen, nach einschlägigem Stand der Technik bezüglich der Hilfsanträge 0a und 0b zu recherchieren. Durch die Ablehnung der hilfsweise von der Klägerin zu 3 und von der Beklagten beantragten Vertagung wäre den Klägerinnen die Möglichkeit entzogen worden, sich vor dem Bundespatentgericht sachgemäß und erschöpfend über die dort verhandelten Fragen zu erklären, die Grundlage der zu treffenden Entscheidung waren. Die zusätzlichen Hilfsanträge, die eine neue „Verteidigungslinie“ bilden, haben die Klägerinnen mit Tatsachen konfrontiert, mit denen sich die Klägerinnen nicht „aus dem Stand“ auseinandersetzen, zu denen sie sachlich fundiert vielmehr nur dann Stellung nehmen konnten, wenn sie angemessene Zeit für Überlegung und Vorbereitung in technischer und rechtlicher Hinsicht hatten. Eine sachgerechte Auseinandersetzung mit den Hilfsanträgen wäre den Klägerinnen keinesfalls bis zum Sitzungsbeginn am folgenden Tag, dem 25. Januar 2019, möglich gewesen, zu dem der Senat ebenfalls zur mündlichen Verhandlung in der vorliegenden Patentnichtigkeitssache geladen hat. Die für eine sachgerechte Auseinandersetzung mit den fraglichen Hilfsanträgen erforderliche Zeit konnte den Klägerinnen auch nicht anders, etwa durch eine Unterbrechung der mündlichen Verhandlung am 24. Januar 2019, in ausreichender Weise zur Verfügung gestellt werden (BGH, Urteil vom 13. Januar 2004, X ZR 212/02, Crimpwerkzeug I, juris, Rn. 28 m. w. N.).

Erhebliche Gründe im Sinne von § 99 Abs. 1 PatG i. V. m. § 227 Abs. 1 ZPO, die eine Vertagung der mündlichen Verhandlung rechtfertigen, sind regelmäßig solche, die den Anspruch auf rechtliches Gehör einer oder mehrerer Parteien berühren und die gerade auch zur Gewährleistung des rechtlichen Gehörs eine Zurückstellung des Beschleunigungs- und Konzentrationsgebots erfordern. So lag es hier aus den geschilderten Gründen. Angesichts der in Art. 103 Abs. 1 GG normierten verfassungsrechtlichen Garantie des Anspruchs auf rechtliches Gehör verblieb dem Senat kein Ermessensspielraum. Zur Gewährung des rechtlichen Gehörs und eines insoweit prozessordnungsgemäßen Verfahrens hätte die mündliche Verhandlung vertagt werden müssen (BGH, Crimpwerkzeug I, a. a. O., Rn. 27 m. w. N.).

c) Die Versäumung der Frist ist durch die Patentinhaberin nicht genügend entschuldigt worden (§ 83 Abs. 4 Satz 1 Nr. 2 PatG).

Die Patentinhaberin hat zwar erklärt, die zusätzlichen Hilfsanträge seien eine Reaktion auf den Verlauf der mündlichen Verhandlung am 24. Januar 2019, bei der erstmals die Frage diskutiert worden sei, ob laut Streitpatent gemäß Merkmal 11.4 alle Daten verschlüsselt werden müssten.

Jedoch ist dies insofern unzutreffend, als eine solche Auslegung des Merkmals 11.4 erstmalig mit dem am 23. Januar 2019, also einen Tag vor der mündlichen Verhandlung, eingegangenen Schriftsatz der Patentinhaberin erfolgt ist und die Patentinhaberin dazu dann erst in der Verhandlung ausführlich dazu vorgetragen hat. Die beiden im Verlauf der Verhandlung von der Patentinhaberin überreichten Hilfsanträge 0a und 0b sowie die entsprechenden Einfügungen in den Text der Hilfsanträge 1 bis 4 sind insbesondere keine Reaktion auf den Verlauf der mündlichen Verhandlung, sondern vielmehr eine Reaktion auf den qualifiziertem Hinweis des Senats vom 12. September 2018. So war dort unter Punkt 2 darauf hingewiesen worden, dass die Druckschrift NK23 i. V. m. dem durch die Druckschriften NK11 bzw. NK20 belegten Fachwissen das drahtlose Endgerät des Anspruchs 11 nahelegen würde. Dieser bereits im qualifizierten Hinweis vom 12. September 2018 geäußerten Auffassung tritt die Patentinhaberin mit den in der mündlichen Verhandlung am 24. Januar 2019 gestellten zusätzlichen

Hilfsanträgen entgegen, indem sie ausführt, dass die Zusatzmerkmale der Hilfsanträge 0a und 0b die Patentfähigkeit der beanspruchten mobilen Endgeräte hinsichtlich der Druckschriften NK23 und NK11 begründen würden, weil damit insbesondere zum Ausdruck käme, dass alle Daten verschlüsselt würden.

Im Blick auf das Erfordernis der genügenden Entschuldigung der Verspätung nach § 83 Abs. 4 Satz 1 Nr. 2 PatG ist auf einen objektivem Sorgfaltsmaßstab abzustellen (BPatG, Urteil vom 14. August 2012, 4 Ni 43/10 (EP), BPatGE 53, 178 = GRUR 2013, 601, Bearbeitungsmaschine, Leitsatz 1, Rn. 34; *Busse/Keukenschrijver*, Patentgesetz, 8. Aufl. 2016, § 83 Rn. 26; *Keukenschrijver*, Patentnichtigkeitsverfahren, 6. Aufl. 2016, Rn. 234; *Benkard/Hall/Nobbe*, Patentgesetz, 11. Aufl. 2015, § 83 Rn. 19). Als ausreichende Entschuldigung wurde angesehen, dass geänderte Hilfsanträge durch ein Ergänzungsgutachten der Gegenseite und einen darauf ergangenen ergänzenden Hinweis des Gerichts (BPatG, Bearbeitungsmaschine, a. a. O.) oder die späte Vorlage von Entgegenhaltungen durch die Gegenseite veranlasst wurden, die eine umfangreiche Überprüfung erforderten (BPatG, Urteil vom 21. September 2015, 5 Ni 30/13 (EP), Verfahren zur Übertragung von Ressourceninformation, juris, Rn. 111).

In diesem Zusammenhang hat die Patentinhaberin in der mündlichen Verhandlung am 24. Januar 2019 weiter erklärt, die jetzt vertretene Auslegung, dass alle Daten verschlüsselt werden müssten, sei ihr erst kurz vor der mündlichen Verhandlung klar geworden, was auch daran liege, dass die beweisbelasteten Klägerinnen diese Problematik bei ihrer Argumentation vorher nicht angesprochen hätten. Aufgrund der in der mündlichen Verhandlung eingereichten NK28, die unvollständig vorgelegt worden sei und keine bibliographischen Daten enthalte, sei eine Vertagung der mündlichen Verhandlung ohnehin erforderlich gewesen.

Mit dieser Erklärung hat die Patentinhaberin bei Anlegung eines objektiven Sorgfaltsmaßstabs indes die Verspätung ihres Vorbringens nicht im Sinne des § 83 Abs. 4 Satz 1 Nr. 2 PatG genügend entschuldigt. Zwar soll die Entschuldigungsmöglichkeit den Parteien ausreichend Möglichkeiten dafür lassen, verspätete Rechercheergebnisse weiterhin einzubeziehen, wenn die

Erkenntnisquellen, auf denen diese Ergebnisse beruhen, nicht so offensichtlich relevant waren, dass sorgfältige Parteien zu einem früheren Zeitpunkt auf sie zurückgegriffen hätten (*Busse/Keukenschrijver*, a. a. O., § 83 Rn. 25; *Keukenschrijver*, a. a. O., Rn. 234 jeweils mit Hinweis auf die Amtl. Begr., BT-Drs. 16/11339, S. 33 = BlfPMZ 2009, 307, 313 ff.). Insofern ist als ausreichende Entschuldigung angesehen worden, dass die geänderten Hilfsanträge durch ein Ergänzungsgutachten der Gegenseite und einen darauf ergangenen ergänzenden Hinweis des Gerichts veranlasst wurden (BPatG, Urteil vom 30. Januar 2014, 4 Ni 38/11 (EP), juris, Rn. 111). Genügend entschuldigt ist eine Verspätung auch dann, wenn die späte Vorlage von Entgegenhaltungen durch die Gegenseite veranlasst worden ist, die eine umfangreiche Überprüfung erforderlich gemacht haben (BPatG, Verfahren zur Übertragung von Ressourceninformation, a. a. O.). Genügend im Sinne des § 83 Abs. 4 Satz 1 Nr. 2 PatG ist eine Entschuldigung auch dann, wenn der Beklagte auf eine geänderte Auffassung des Senats reagierte, zu der dieser auf Grund des Vortrags des Klägers erst in der mündlichen Verhandlung gelangt war (BPatG, Urteil vom 29. April 2015, 4 Ni 26/13 (EP), juris, Rn. 143). Als Entschuldigungsgrund nicht anerkannt werden kann dagegen das Vorbringen einer Partei, erst vor wenigen Tagen auf ein Dokument gestoßen sein (BPatG, Urteil vom 13. April 2011, 4 Ni 16/10 (EU), juris, Rn. 243; zustimmend *Keukenschrijver*, a. a. O., Rn. 234 und *Busse/Keukenschrijver*, a. a. O., § 83 Rn. 27).

Mit ihrer Erklärung in der mündlichen Verhandlung am 24. Januar 2019, die jetzt vertretene Auslegung, dass alle Daten verschlüsselt werden müssten, sei ihr erst kurz vor der mündlichen Verhandlung klar geworden, versucht die Patentinhaberin die verspätete Einreichung ihrer zusätzlichen Hilfsanträge in genau dieser Weise zu entschuldigen. Als Entschuldigungsgrund kann dieses Vorbringen in Fortführung der zitierten Rechtsprechung und Literatur indes nicht anerkannt werden, weil die Patentinhaberin seit dem Zugang des qualifizierten Hinweises vom 12. September 2018 am 17. September 2018 genug Zeit hatte, sich über die Auslegung, dass alle Daten verschlüsselt werden müssen, klar zu werden. Hinzu tritt, dass die Klägerin zu 1, die das Lehrbuch, aus dem der Auszug NK28 stammt, mitgebracht hatte, der Beklagten in der mündlichen Verhandlung am 24. Januar 2019 angeboten hat, das Buch zur Prüfung zur Verfügung zu stellen, zumal der

Auszug NK28 nach Aussage der Klägerin zu 1 ohnehin bloß ergänzende Hinweise auf das präsente bereits früher im Verfahren genannte Fachwissen geben sollte.

Durch die Vorlage der von der Klägerin zu 3 in der mündlichen Verhandlung am 24. Januar 2019 vorgelegten NK28 wäre eine Vertagung der mündlichen Verhandlung nicht erforderlich gewesen, weil der Beklagten durch die Ablehnung der Vertagung aus diesem Grund nicht die Möglichkeit entzogen worden wäre, sich vor dem Bundespatentgericht sachgemäß und erschöpfend über die dort verhandelten Fragen zu erklären, die Grundlage der zu treffenden Entscheidung waren, und auch im Übrigen keine erheblichen Gründe ersichtlich sind, die eine Vertagung wegen der Vorlage der NK28 erforderlich gemacht hätte.

d) Die Patentinhaberin ist in dem qualifizierten Hinweis vom 12. September 2018, der ihr am 17. September 2018 zugegangen ist, über die Folgen einer Fristversäumung belehrt worden.

2. Auch die Gewährung einer Schriftsatzfrist (§ 99 Abs. 1 PatG i. V. m. § 283 ZPO) hätte eine Vertagung nicht ersetzen können, da diese nur eine (einseitige) Äußerung durch die Klägerinnen und nicht eine sich daran anschließende Rückäußerung der Beklagten (beispielsweise zu einem im Hinblick auf die Hilfsanträge 0a und 0b neu eingeführten Stand der Technik) ermöglicht (BPatG, Urteil vom 16. Oktober 2012, 3 Ni 11/11 (EP), beschichtetes Schneidwerkzeug, juris, Rn. 67).

3. Der Senat übt das ihm nach § 83 Abs. 4 Satz 1 PatG eingeräumte Ermessen durch Zurückweisung der Verteidigung des Streitpatents nach Maßgabe der zusätzlich erstmals in der mündlichen Verhandlung gestellten Hilfsanträge aus. Unter Abwägung der für und gegen eine Präklusion sprechenden Gründe, insbesondere des Umstands, dass sich die Zurückweisung gegen die Schutzrechtsinhaberin richtet, entspricht diese Entscheidung der herrschenden Rechtsauffassung, wonach in normal gelagerten Fällen aus Gründen der Prozessökonomie und Rechtssicherheit eine Zurückweisung zu erfolgen hat

(BPatG, Urteil vom 25. April 2012, 5 Ni 28/10 (EP), Wiedergabeschutzverfahren, juris, Rn. 134; *Benkard/Hall/Nobbe*, a. a. O., § 83 Rn. 22). Eine Ausnahme hiervon ist Fällen vorzubehalten, in denen die rechtlichen Voraussetzungen einer Zurückweisung zweifelhaft sind oder aus sonstigen Gründen der Billigkeit Anlass dazu besteht, verspätetes Vorbringen zu berücksichtigen (BPatG, Wiedergabeschutzverfahren, a. a. O.; BPatG, Urteil vom 12. März 2013, 4 Ni 13/11, Dichtungsring, juris, Rn. 84 m. w. N.). Eine derartige Fallgestaltung liegt hier nicht vor.

IV.

Die Kostenentscheidung beruht auf § 84 Abs. 2 PatG i. V. m. § 91 Abs. 1 Satz 1 ZPO.

Die Entscheidung über die vorläufige Vollstreckbarkeit folgt aus § 99 Abs. 1 PatG i. V. m. § 709 Satz 1 und 2 ZPO.

V.

Rechtsmittelbelehrung

Gegen dieses Urteil ist das Rechtsmittel der Berufung gemäß § 110 PatG statthaft.

Die Berufung ist innerhalb eines Monats nach Zustellung des in vollständiger Form abgefassten Urteils - spätestens nach Ablauf von fünf Monaten nach Verkündung - durch einen in der Bundesrepublik Deutschland zugelassenen Rechtsanwalt oder Patentanwalt schriftlich beim Bundesgerichtshof, Herrenstraße 45a, 76133 Karlsruhe, einzulegen.

Die Berufungsschrift muss

- die Bezeichnung des Urteils, gegen das die Berufung gerichtet ist, sowie
- die Erklärung, dass gegen dieses Urteil Berufung eingelegt werde,

enthalten. Mit der Berufungsschrift soll eine Ausfertigung oder beglaubigte Abschrift des angefochtenen Urteils vorgelegt werden.

Auf die Möglichkeit, die Berufung nach § 125a PatG in Verbindung mit § 2 der Verordnung über den elektronischen Rechtsverkehr beim Bundesgerichtshof und Bundespatentgericht (BGH/BPatGERVV) auf elektronischem Weg beim Bundesgerichtshof einzulegen, wird hingewiesen (www. bundesgerichtshof.de/erv.html).

Guth Dr. Himmelmann Dr. Friedrich Dr. Zebisch Dr. Kapels