BUNDESPATENTGERICHT

23 W (pat) 25/17

(Aktenzeichen)

B E S C H L U S S

In der Beschwerdesache

…

betreffend die Patentanmeldung 10 2013 019 870.4

hat der 23. Senat (Technischer Beschwerdesenat) des Bundespatentgerichts am 23. Januar 2018 unter Mitwirkung des Vorsitzenden Richters Dr. Strößner und der Richter Brandt, Dr. Friedrich und Dr. Himmelmann

ECLI:DE:BPatG:2018:230118B23Wpat25.17.0

beschlossen:

1. Der Beschluss der Prüfungsstelle für Klasse H04L des Deutschen Patent- und Markenamts vom 11. Januar 2016 wird aufgehoben.
2. Die Sache wird zur weiteren Prüfung an das Deutsche Patent- und Markenamt zurückverwiesen.

G r ü n d e

I.

Die vorliegende Anmeldung mit dem Aktenzeichen 10 2013 019 870.4 und der Bezeichnung „Authentifizierungs- und/oder Identifikationsverfahren in einem Kommunikationsnetzwerk“ wurde am 28. November 2013 beim Deutschen Patent- und Markenamt eingereicht.

Die Prüfungsstelle für Klasse H04L hat im Prüfungsverfahren auf den Stand der Technik gemäß den Druckschriften

D1 Menezes, J. u. a.: Handbook of applied cryptography. Boca Raton, u. a., CRC Press, 1997, ISBN:0-8493-8523-7, S. 397 - 403.
D2 DE 10 2011 101 711 A1
D3 US 6 636 973 B1
D4 DE 10 2011 085 538 A1

verwiesen und im einzigen Prüfungsbescheid vom 10. Oktober 2014 ausgeführt, dass das beanspruchte Verfahren als ein dem Patentierungsausschluss unterliegendes Programm für Datenverarbeitungsanlagen anzusehen sei, das zwar auf technischem Gebiet liege, aber keine Anweisungen enthalte, die der Lösung eines

konkreten technischen Problems mit technischen Mitteln diene, denn es berücksichtige nicht die technischen Gegebenheiten der Kommunikationseinrichtung und der Datenbank, sondern beschränke sich darauf, im Stand der Technik bekannte technische Mittel einzusetzen, um Daten zusammenzustellen, zu verarbeiten und zu übermitteln, so dass es nicht über die bloße Übermittlung und Verarbeitung von Daten hinausgehe. Gleiches gelte für das Verfahren des Nebenanspruchs 12.

Zudem beträfen sämtliche Definitionen der Änderbarkeit der Zeichen in Anspruch 1 nicht-technische Merkmale. Diese seien für die Beurteilung der erfinderischen Tätigkeit jedoch unbeachtlich, und daher könne der Fachmann das Verfahren gemäß den noch verbleibenden Merkmalen des Anspruchs 1 der Druckschrift D1 entnehmen, wobei bezüglich der grundlegenden Idee der Anmeldung betreffend den Einsatz von Codewörtern mit einem statischen und einem dynamischen Anteil auf die Druckschriften D2 bis D4 zu verweisen sei.

Mit Eingabe vom 13. Februar 2015 hat der Anmelder ausgeführt, dass das Verfahren nach Anspruch 1 ein technisches Problem mit technischen Mitteln löse, denn es würden technische Mittel zur Authentifizierung und/oder Identifikation eingesetzt. So sei anspruchsgemäß ein Kommunikationsnetzwerk aus einer Kommunikationseinrichtung und einer zentralen Datenbank, also zwei unabhängigen technischen Komponenten, vorgesehen. Auch der in der Kommunikationseinrichtung bzw. in der zentralen Datenbank bereitgestellte Authentifizierungsschlüssel an sich habe technischen Charakter, denn es müsse in erfinderischer Weise überlegt werden, welche Zeichen in einer Zeichenfolge veränderbar bzw. unveränderbar seien. Bei einer Software hingegen würde ein Schlüssel einen Programmcode beinhalten, über den eine bestimmte Funktion ausgeübt werde, was bei dem beanspruchten Verfahren nicht der Fall sei, da der Schlüssel anspruchsgemäß keine Programmanweisungen ausübe, sondern lediglich als Authentifizierungsschlüssel herangezogen würde. Schließlich erfolge auch das Übertragen und Abgleichen der in der zentralen Datenbank und der Kommunikationseinrichtung hinterlegten Schlüssel mit technischen Mitteln. Zudem sei auch das der Erfindung

zugrundeliegende Problem technischer Natur, denn es bestehe darin, die Sicherheit bei einer Authentifikation eines Gerätes, eines Dienstes, einer Person und/oder eines Geldmittels zu erhöhen. Darüber hinaus werde das beanspruchte Verfahren dem Fachmann auch nicht durch die Dokumente D1 bis D4 nahegelegt.

Da keine Anhörung beantragt war, hat die Prüfungsstelle die Anmeldung daraufhin durch Beschluss vom 11. Januar 2016 mit der Begründung, dass der geltende Patentanspruch 1 unter den Patentierungsausschluss für Programme für Datenverarbeitungsanlagen (§ 1 Abs. 3 Nr. 3, Abs. 4 PatG) falle, zurückgewiesen.

Gegen diesen dem Vertreter des Anmelders am 14. Januar 2016 zugestellten Beschluss richtet sich die am 12. Februar 2016 beim Deutschen Patent- und Markenamt eingegangene Beschwerde mit der weiteren Eingabe vom 24. März 2016. Darin wird sinngemäß beantragt,

1. den Beschluss der Prüfungsstelle für Klasse H04L des Deutschen Patent- und Markenamts vom 11. Januar 2016 aufzuheben,
2. auf Grundlage der ursprünglichen Unterlagen ein Patent zu erteilen,
3. eine mündliche Verhandlung anzuberaumen, sofern eine Zurückweisung der Beschwerde in Erwägung gezogen wird.

Die geltenden selbständigen Ansprüche 1 und 12 haben folgenden Wortlaut:

1. Verfahren zur Authentifizierung und/oder Identifikation eines Gerätes, eines Dienstes, einer Person und/oder eines Geldmittels in einem Kommunikationsnetzwerk, bestehend aus einer Kommunikationseinrichtung und einer zentralen Datenbank, zwischen denen eine Authentifizierungsabfrage durchgeführt wird, umfassend die Schritte:

– Bereitstellen eines ersten Schlüssels in der Kommunikationseinrichtung, der wenigstens eine Zeichenfolge umfasst, bestehend aus
  - einzelnen oder mehreren lokal veränderbaren Zeichen, die sich in Abhängigkeit eines internen Einflusses, eines externen Einflusses, eines Algorithmus, einer Regel und/oder einer Anweisung in der Kommunikationseinrichtung zwischen zwei Authentifizierungszeitpunkten dynamisch verändern,
  - einzelnen oder mehreren lokal unveränderbaren Zeichen in dieser oder einer weiteren lokal hinterlegten Zeichenfolge, die zwischen zwei Authentifizierungszeitpunkten in der Kommunikationseinrichtung statisch bleiben,
– Bereitstellen eines zweiten Schlüssels in der zentralen Datenbank, der eine Zeichenfolge umfasst, bestehend aus
  - einzelnen oder mehreren zentral veränderbaren Zeichen in dieser oder einer weiteren Zeichenfolge, die den lokal unveränderbaren Zeichen oder der Zeichenfolge der Kommunikationseinrichtung des letzten Authentifizierungszeitpunktes entsprechen,
  - einzelnen oder mehreren zentral unveränderbaren Zeichen, die den lokal veränderbaren Zeichen oder der Zeichenfolge der Kommunikationseinrichtung des letzten Authentifizierungszeitpunktes entsprechen,
– Übertragen und Abgleich der in der zentralen Datenbank und der Kommunikationseinrichtung hinterlegten Schlüssel,

dadurch gekennzeichnet, dass eine positive Authentifizierung und/oder Identifikation des Gerätes, des Dienstes, der Person und/oder des Geldmittels beim Authentifizierungszeitpunkt dann erfolgt, wenn zumindest folgende Merkmale erfüllt sind:

i. zumindest teilweise Übereinstimmung der lokal unveränderbaren Zeichen oder Zeichenfolge im Schlüssel der Kommunikationseinrichtung mit den entsprechenden zentral veränderbaren Zeichen oder Zeichenfolge im Schlüssel der zentralen Datenbank,

ii. zumindest teilweise fehlende Übereinstimmung der lokal veränderbaren Zeichen oder Zeichenfolge im Schlüssel der Kommunikationseinrichtung mit den entsprechenden zentral unveränderbaren Zeichen oder Zeichenfolge im letzten Schlüssel der zentralen Datenbank,

wobei die lokal veränderbaren Zeichen oder Zeichenfolge zwischen zwei Authentifizierungszeitpunkten nur in der Kommunikationseinrichtung, nicht jedoch in der zentralen Datenbank und die zentral veränderbaren Zeichen oder Zeichenfolge nur in der zentralen Datenbank, aber nicht in der Kommunikationseinrichtung veränderbar sind.

12. Verfahren zur Authentifizierung und/oder Identifikation eines Gerätes, eines Dienstes, einer Person und/oder eines Geldmittels in einem Kommunikationsnetzwerk, bestehend aus einer Kommunikationseinrichtung und einer zentralen Datenbank, zwischen denen eine Authentifizierungsabfrage durchgeführt wird, umfassend die Schritte:

a. Bereitstellen eines ersten Schlüssels in der zentralen Datenbank, der wenigstens eine Zeichenfolge umfasst, bestehend aus

   1. einzelnen oder mehreren zentral veränderbaren Zeichen, die sich in Abhängigkeit eines internen Einflusses, eines externen Einflusses, eines Algorithmus, einer Regel und/oder einer Anweisung in der zentralen

Datenbank zwischen zwei Authentifizierungszeitpunkten dynamisch verändern,

2. einzelnen oder mehreren zentral unveränderbaren Zeichen in dieser oder einer weiteren zentral hinterlegten Zeichenfolge, die zwischen zwei Authentifizierungszeitpunkten in der zentralen Datenbank statisch bleiben,

b. Bereitstellen eines zweiten Schlüssels in der Kommunikationseinrichtung, der eine Zeichenfolge umfasst, bestehend aus

1. einzelnen oder mehreren lokal veränderbaren Zeichen in dieser oder einer weiteren Zeichenfolge, die den zentral unveränderbaren Zeichen oder der Zeichenfolge der zentralen Datenbank des letzten Authentifizierungszeitpunktes entsprechen,
2. einzelnen oder mehreren lokal unveränderbaren Zeichen, die den zentral veränderbaren Zeichen oder der Zeichenfolge der zentralen Datenbank des letzten Authentifizierungszeitpunktes entsprechen,

c. Übertragen und Abgleich der in der zentralen Datenbank und der Kommunikationseinrichtung hinterlegten Schlüssel,

dadurch gekennzeichnet, dass eine positive Authentifizierung und/oder Identifikation des Gerätes, des Dienstes, der Person und/oder des Geldmittels beim Authentifizierungszeitpunkt dann erfolgt, wenn zumindest folgende Merkmale erfüllt sind:

i. zumindest teilweise Übereinstimmung der zentral unveränderbaren Zeichen oder Zeichenfolge im Schlüssel der zentralen Datenbank mit den entsprechenden lokal veränderbaren Zeichen oder Zeichenfolge im Schlüssel der Kommunikationseinrichtung,

ii. zumindest teilweise fehlende Übereinstimmung der zentral veränderbaren Zeichen oder Zeichenfolge im Schlüssel der zentralen Datenbank mit den entsprechenden lokal unveränderbaren Zeichen oder Zeichenfolge im letzten Schlüssel der Kommunikationseinrichtung,

wobei die zentral veränderbaren Zeichen oder Zeichenfolge zwischen zwei Authentifizierungszeitpunkten nur in der zentralen Datenbank, nicht jedoch in der Kommunikationseinrichtung und die lokal veränderbaren Zeichen oder Zeichenfolge nur in der Kommunikationseinrichtung, aber nicht in der zentralen Datenbank veränderbar sind.

Hinsichtlich der abhängigen Ansprüche 2 bis 11, 13 und 14 sowie der weiteren Einzelheiten wird auf den Akteninhalt verwiesen.

II.

Die form- und fristgerecht erhobene Beschwerde ist zulässig und insoweit begründet, als der Beschluss der Prüfungsstelle für Klasse H04L vom 11. Januar 2016 aufzuheben ist, denn die Verfahren der selbständigen Ansprüche 1 und 12 fallen nicht unter den Patentierungsausschluss für Programme für Datenverarbeitungsanlagen (§ 1 Abs. 3 Nr. 3, Abs. 4 PatG). Da zudem die in den Ansprüchen erfolgten Definitionen der Änderbarkeit der Zeichen entgegen den Ausführungen der Prüfungsstelle einen für die Beurteilung der erfinderischen Tätigkeit zu berücksichtigenden Kernaspekt der beanspruchten Lehre darstellen, und diesbezüglich bisher keine Recherche erfolgt ist, wird die Anmeldung zur weiteren Bearbeitung an das Deutsche Patent- und Markenamt zurückverwiesen (§ 79 Abs. 3 Satz 1 Nr. 1 und 2 PatG).

1. Die Anmeldung betrifft ein Verfahren zur Authentifizierung und/oder Identifikation eines Gerätes, eines Dienstes, einer Person und/oder eines Geldmittels in einem Kommunikationsnetzwerk, das aus einer Kommunikationseinrichtung und einer zentralen Datenbank besteht, zwischen denen eine Authentifizierungsabfrage durchgeführt wird.

Nach den Ausführungen in der Beschreibungseinleitung sind verschiedene Sicherheitsverfahren zur Durchführung eines Datenaustauschs in einem Netzwerk zwischen unterschiedlichen Netzwerkteilnehmern bekannt. So identifiziere bei einem bekannten Sicherheitsverfahren ein dynamischer Sicherheitscode kryptografisch eine mobile Kommunikationseinrichtung eines Benutzers in einem Netzwerk. Die Dynamik des Codes bestehe dabei im Austausch des Sicherheitselements nach jeder erfolgten Authentifizierung. Bei diesem Verfahren handele sich also um dynamisch aufeinanderfolgende statische Sicherheitscodes. Die Codes an sich blieben aber statisch und würden nicht fortlaufend verändert, sondern insgesamt ersetzt, also neu berechnet und herausgegeben. Dabei würden unterschiedliche Sicherheitsabfragen zwischen dem Dienstleistungsanbieter und dem Benutzer bzw. dessen Gerät durchgeführt.

Viele bekannte Sicherheitsverfahren sähen starre Sicherheitsanfragen vor, wie bspw. die Abfrage von Passwörtern oder PIN-Nummern. Daneben gebe es Verfahren, die mit einem sich periodisch oder gemäß einem Algorithmus ändernden dynamischen Code arbeiteten, wobei aber nur dessen Generierung dynamisch sei, denn nach der dynamischen Generierung bleibe der Code statisch und könne deshalb nur einmal angewendet werden. Er werde somit bei jeder weiteren Authentifikation wieder neu berechnet. Solche Verfahren seien von einem Angreifer überwindbar, wenn er widerrechtlich Zugriff auf die entsprechende Datenbank oder den Algorithmus erhalte. Biometrische Merkmale würden deshalb häufig zur Identifizierung herangezogen, seien allerdings anfällig für Fälschungen und Kopien. Daneben böten diese Verfahren keine ausreichende Sicherheit, wenn ein Angreifer Zugriff auf eine Kommunikationseinrichtung, bspw. ein Smartphone, er-

halte und er dieses für die Durchführung von Diensten, bspw. Finanztransaktionen, missbrauche. Ein hinsichtlich unberechtigter Zugriffe auf die zentrale oder lokale Datenbank weniger empfindliches Sicherheitssystem, das für die Autorisierung von Diensten oder Geldmitteln herangezogen werden könne, sei daher wünschenswert, *vgl. Beschreibungsseite 1 bis Seite 3, erster Absatz.*

Vor diesem Hintergrund liegt der Anmeldung als technisches Problem die Aufgabe zugrunde, ein alternatives und verbessertes Verfahren zur Authentifizierung und/oder Identifikation eines Gerätes, eines Dienstes, einer Person und/oder eines Geldmittels in einem Kommunikationsnetzwerk bereit zu stellen, *vgl. Beschreibungsseite 3, zweiter Absatz.*

Diese Aufgabe wird durch die Verfahren der selbständigen Ansprüche 1 und 12 gelöst.

Diese haben die Durchführung einer Authentifizierungsabfrage zwischen einer zentralen Datenbank, bspw. einem stationären Serversystem, und einer Kommunikationseinrichtung, bspw. einem Smartphone, zum Gegenstand.

Dazu werden nach Anspruch 1 in der Kommunikationseinrichtung ein erster Schlüssel, der wenigstens eine lokal (in der Kommunikationseinrichtung) hinterlegte Zeichenfolge umfasst, und in der zentralen Datenbank ein zweiter Schlüssel, der wenigstens eine zentral (in der zentralen Datenbank) hinterlegte Zeichenfolge umfasst, bereitgestellt. Der lokal hinterlegte erste Schlüssel besteht aus lokal veränderbaren Zeichen, die nur in der Kommunikationseinrichtung veränderbar sind und sich zwischen zwei Authentifizierungszeitpunkten dynamisch verändern, und lokal unveränderbaren Zeichen, die zwischen zwei Authentifizierungszeitpunkten in der Kommunikationseinrichtung statisch bleiben. In ähnlicher Weise besteht der zentral hinterlegte zweite Schlüssel aus zentral veränderbaren Zeichen, die nur in der zentralen Datenbank veränderbar sind, und zentral unveränderbaren Zeichen. Dabei basiert dieser zweite Schlüssel insofern auf dem vorhergehenden Schlüs-

sel, als die zentral veränderbaren Zeichen des zweiten Schlüssels den lokal unveränderbaren Zeichen der Kommunikationseinrichtung des letzten Authentifizierungszeitpunkts entsprechen und die zentral unveränderbaren Zeichen des zweiten Schlüssels den lokal veränderbaren Zeichen der Kommunikationseinrichtung des letzten Authentifizierungszeitpunkts entsprechen.

In einem weiteren Verfahrensschritt erfolgt ein Übertragen und ein Abgleich der in der zentralen Datenbank und der Kommunikationseinrichtung hinterlegten Schlüssel. Eine positive Authentifizierung liegt dann vor, wenn die lokal unveränderbaren Zeichen im Schlüssel der Kommunikationseinrichtung mit den entsprechenden zentral veränderbaren Zeichen im Schlüssel der zentralen Datenbank zumindest teilweise übereinstimmen und wenn die lokal veränderbaren Zeichen im Schlüssel der Kommunikationseinrichtung mit den entsprechenden zentral unveränderbaren Zeichen im letzten Schlüssel der zentralen Datenbank zumindest teilweise nicht übereinstimmen.

Der selbständige Anspruch 12 betrifft das entsprechende Authentifizierungsverfahren für den Fall, dass die Rollen von Kommunikationseinrichtung und zentraler Datenbank vertauscht sind.

Ein Beispiel für das beanspruchte Authentifizierungsverfahren findet sich in der Beschreibung von Fig. 2 auf den Seiten 21 und 22 der Anmeldung. Dabei sind zunächst lokal und zentral der gleiche erste und zweite Schlüssel hinterlegt, bspw. die Zahlenfolge 1, **2**, **3**, 4, 5, **6**. Von dieser Zahlenfolge sind die Zahlen 1, 4 und 5 lokal veränderbar und zentral unveränderbar, wohingegen die Zahlen **2**, **3** und **6** **lokal unveränderbar** und **zentral veränderbar** sind. In einem ersten Schritt wird die Zahlenfolge von der Kommunikationseinrichtung an die zentrale Datenbank übermittelt, wo die zentral veränderbaren Zahlen 2, 3 und 6 bspw. durch 0 ersetzt werden. Die geänderte Zahlenfolge lautet nun 1, **0**, **0**, 4, 5, **0**. Sie wird zentral gespeichert und in einem zweiten Schritt wieder auf die Kommunikationseinrichtung übertragen. In der Kommunikationseinrichtung werden die lokal veränderbaren

Zahlen 1, 4 und 5 bspw. in 3, 6 und 7 geändert. Die geänderte Zahlenfolge 3, **0**, **0**, 6, 7, **0** wird in einem dritten Schritt wieder an die zentrale Datenbank gesendet und dort authentifiziert.

Hier setzt das Verfahren des Anspruchs 1 ein, denn jetzt werden der zentral gespeicherte letzte Schlüssel (Zahlenfolge 1, **0**, **0**, 4, 5, **0**), sowie der aktuelle Schlüssel (Zahlenfolge 3, **0**, **0**, 6, 7, **0**) dahingehend überprüft, ob die lokal unveränderbaren Zahlen (**0**, **0**, **0**) des aktuellen Schlüssels (3, **0**, **0**, 6, 7, **0**) mit den zentral veränderbaren Zahlen des zentral gespeicherten letzten Schlüssels (1, **0**, **0**, 4, 5, **0**) übereinstimmen und ob die lokal veränderbaren Zahlen (3, 6, 7) des aktuellen Schlüssels (3, **0**, **0**, 6, 7, **0**) nicht mit den zentral unveränderbaren Zahlen (1, 4, 5) des zentral gespeicherten letzten Schlüssels (1, **0**, **0**, 4, 5, **0**) übereinstimmen. Trifft dies zu, so erfolgt eine positive Authentifizierung.

Die dynamische Änderung der Schlüssel kann dabei interne Faktoren wie Prozessorauslastung, Zeitwertedifferenz usw. und externe Faktoren wie Temperaturänderung, Positionsänderung, Häufigkeit der Nutzung von Kontakten usw. berücksichtigen.

Insbesondere soll die Kombination lokal veränderbarer und lokal unveränderbarer Zeichen bzw. zentral veränderbarer und zentral unveränderbarer Zeichen (bzw. Zeichenfolgen) ein hohes Maß an Sicherheit für die Authentifizierung und/oder Identifikation eines Gerätes, eines Dienstes, einer Person oder eines Geldmittels gewährleisten.

2. Die Ansprüche 1 bis 14 sind die ursprünglichen Ansprüche und folglich hinsichtlich der Ursprungsoffenbarung zulässig.

3. Als Fachmann ist hier ein berufserfahrener Informatiker mit Hochschulabschluss und guten Kenntnissen von kryptographischen und Authentifizierungsverfahren zu definieren.

4. Nach der Rechtsprechung des Bundesgerichtshofs genügt ein Verfahren, dessen Gegenstand die Abarbeitung von Verfahrensschritten mit Hilfe elektronischer Datenverarbeitung ist, dem Technizitätserfordernis (§ 1 Abs. 1 PatG) bereits dann, wenn es der Verarbeitung, Speicherung oder Übermittlung von Daten mittels eines technischen Geräts dient. Für das Technizitätserfordernis ist unerheblich, ob der Gegenstand des Patents neben technischen Merkmalen auch nichttechnische aufweist und welche dieser Merkmale die beanspruchte Lehre prägen (BGH GRUR 2011, 610 - Webseitenanzeige).

Demnach liegen die Verfahren der selbständigen Ansprüche 1 und 12, die sich auf die Authentifizierung und/oder Identifikation eines Gerätes, eines Dienstes, einer Person und/oder eines Geldmittels in einem Kommunikationsnetzwerk, bestehend aus einer Kommunikationseinrichtung und einer zentralen Datenbank, zwischen denen eine Authentifizierungsabfrage durchgeführt wird, beziehen, auf technischem Gebiet.

Zudem muss eine Lehre, die ein durch ein Datenverarbeitungsprogramm verwirklichtes Verfahren zum Gegenstand hat, wegen des Patentierungsausschlusses für Computerprogramme als solche (§ 1 Abs. 3 Nr. 3 und Abs. 4 PatG) über die für die Patentfähigkeit unabdingbare Technizität hinaus verfahrensbestimmende Anweisungen enthalten, die der Lösung eines konkreten technischen Problems mit technischen Mitteln dienen. Ob ein konkretes technisches Problem durch eine Erfindung mit technischen Mitteln gelöst wird, ist dabei durch Auslegung des Patentanspruchs objektiv danach zu bestimmen, was die Erfindung tatsächlich leistet. U. a. kann von einem zur Lösung eines technischen Problems eingesetzten technischen Mittel dann gesprochen werden, wenn der Ablauf eines zur Problemlösung eingesetzten Datenverarbeitungsprogramms durch technische Gegebenheiten außerhalb der Datenverarbeitungsanlage bestimmt wird oder wenn die Lösung darin besteht, ein Datenverarbeitungsprogramm so auszugestalten, dass es auf die technischen Gegebenheiten der Datenverarbeitungsanlage Rücksicht nimmt.

Die der Anmeldung als technisches Problem zugrundeliegende objektive Aufgabe, besteht darin, ein Verfahren zur Authentifizierung und/oder Identifikation eines Gerätes, eines Dienstes, einer Person und/oder eines Geldmittels in einem Kommunikationsnetzwerk bereit zu stellen, das bezüglich unberechtigter Zugriffe auf die zentrale oder lokale Datenbank unempfindlich ist (*vgl. Beschreibungsseite 2, letzter Absatz bis Seite 3, zweiter Absatz).* Dies stellt ein konkretes technisches Problem dar.

Wie bereits ausgeführt, erfolgt bei den beanspruchten Verfahren eine Authentifizierungsabfrage zwischen einer zentralen Datenbank, bspw. einem stationären Serversystem, und einer Kommunikationseinrichtung, bspw. einem Smartphone. Die dazu in der Kommunikationseinrichtung und der zentralen Datenbank eingesetzten Authentifizierungsschlüssel zeichnen sich dadurch aus, dass sie aus einer Zeichenfolge bestehen, deren einer Teil zentral unveränderbar bzw. nur lokal veränderbar und deren anderer Teil lokal unveränderbar bzw. nur zentral veränderbar ist, so dass sie zwischen zwei Authentifizierungszeitpunkten einen statischen und einen sich dynamisch ändernden Anteil aufweisen. Der aktuelle Authentifizierungsschlüssel setzt sich folglich aus statischen Zeichen aus dem vorhergehenden Schlüssel und dynamisch geänderten Zeichen zusammen, wobei deren verbotene oder zwingend erforderliche Änderung im Rahmen der Authentifizierung geprüft wird. Insbesondere durch die Kombination lokal veränderbarer und lokal unveränderbarer Zeichen bzw. zentral veränderbarer und zentral unveränderbarer Zeichen (bzw. Zeichenfolgen) soll ein hohes Maß an Sicherheit für die Authentifizierung und/oder Identifikation gewährleistet werden, die zusätzlich durch die Art der dynamischen Änderung vorgegeben wird, denn gemäß dem beanspruchten Verfahren ändern sich die Zeichen in Abhängigkeit eines internen Einflusses, eines externen Einflusses, eines Algorithmus, einer Regel und/oder einer Anweisung zwischen zwei Authentifizierungszeitpunkten dynamisch. Dies ist in der Beschreibung (Seite 6, zweiter Absatz bis Seite 7, erster Absatz) folgendermaßen erläutert:

„Externe oder interne Einflüsse basieren vorzugsweise auf physikalischen oder chemischen Eigenschaften oder Prozessen. Ein interner Einfluss umfasst beispielsweise einen Zeitgeber, den Zeitpunkt der letzten Authentifizierung/en, eine Differenz zwischen zwei Zeitwerten, einen Impuls oder einen parameterabhängigen Algorithmus, eine spezielle Konfiguration (z. B. Version eines Betriebssystems, geladene mobile Softwarepakete (APPs), benutzte Apps oder offene Anwendungen). Daneben können die Einflüsse auch eine individuelle Modifikation (z. B. eine zusätzliche SD Karte, ein RAM-Upgrade) oder anwendungsspezifische bzw. anwenderabhängige Merkmale (z. B. typische Prozessorauslastung, Betriebstemperatur) umfassen. Ein externer Einfluss umfasst beispielsweise eine Temperaturänderung, eine Druckänderung, die Anzahl oder Impulsstärke von Erschütterungen, eine Positionsänderung eines sich bewegenden Teilnehmers, typische Verhaltens- oder Bedienungsmerkmale eines Nutzers (z. B. Anzahl paralleler Kontakte mit anderen Benutzern, Kontakte pro Zeitraum, welche Kontakte = Kontaktgruppe, wobei diese sich je nach Tageszeit signifikant ändern kann), Häufigkeit der Nutzung, ebenfalls in Abhängigkeit von der Uhrzeit/eines Zeitraumes, Sprechlautstärke, andere Vorlieben, wie bevorzugte Musik, bevorzugte APPs, bevorzugte Worte und Wortkürzel. Eine Regel umfasst beispielsweise die Anwendung einer Grundrechenregel, Herunterzählen oder Heraufzählen eines Wertes oder einer Zahl, eines allgemeinen Algorithmus oder auch das Pendeln innerhalb von Grenzwerten und das Verschieben der Zahlenposition. Eine Anweisung umfasst beispielsweise eine Vergrößerung oder Verminderung eines Guthabenbetrages um einen bestimmten Wert, das Aufbrauchen eines Guthabenbetrags, eine festgelegte Änderung einer Zahlenfolge oder die Zuordnung eines Wertes. Beispielsweise kann die Zeichenfolge einen Geldbetrag umfassen, der vollständig als Bezahlungsmittel verbraucht wird, wobei die Zahlenfolge nach der Transaktion entwertet ist.“

Solche dynamischen Veränderungen, die lokal auf der Kommunikationseinrichtung laufen, sind von der zentralen Datenbank nicht vorhersehbar und können daher auch nicht entschlüsselt werden. Umgekehrt sind dynamische Veränderungen der zentralen Datenbank nur dieser bekannt, da die entsprechenden Regeln oder Anweisungen nicht in der lokalen Kommunikationseinrichtung hinterlegt sind. Die Sicherheit ist daher auch in dem Fall gewährleistet, dass ein Angreifer Zugriff auf die Kommunikationseinrichtung, bspw. ein Smartphone, erhält.

Damit betreffen die Verfahren der Ansprüche 1 und 12 nicht nur den Programmablauf in einer Datenverarbeitungsanlage und die bloße Verarbeitung von Daten als solche, sondern insbesondere die Bereitstellung sicherer Authentifizierungs- bzw- Identifikationsschlüssel durch eine dynamische Veränderung der Schlüssel entsprechend den obigen Vorgaben. Die Eigenschaften der Kommunikationseinrichtung und der zentralen Datenbank beeinflussen somit die Ausgestaltung der Schlüssel insofern, als technische Gegebenheiten Berücksichtigung finden.

Der Ausschlusstatbestand des § 1 Abs. 3 Nr. 3 PatG greift daher nicht (vgl. BGH, Urteil vom 25. Oktober 2016, X ZR 68/15, juris, Rn. 38, 39).

5. Ein Kernaspekt der anspruchsgemäßen Lösung der Aufgabe besteht darin, dass sowohl in der Kommunikationseinrichtung als auch in der zentralen Datenbank wenigstens ein Schlüssel hinterlegt ist, der aus nur lokal veränderbaren und lokal unveränderbaren Zeichen bzw. nur zentral veränderbaren und zentral unveränderbaren Zeichen (bzw. Zeichenfolgen) zusammengesetzt ist. Bestimmte Zeichen bleiben somit während bzw. zwischen zwei Authentifizierungszeitpunkten unveränderbar, werden jedoch bei einer nachfolgenden Authentifizierung wieder verändert. Dabei ist die Vorschrift, nach der die nur lokal veränderbaren Zeichen geändert werden, der zentralen Datenbank unbekannt, und umgekehrt kennt die Kommunikationseinrichtung nicht die Vorschrift, nach der die nur zentral veränderbaren Zeichen geändert werden. Da diese Veränderungen nach jeder Authentifizierung in der jeweils anderen Datenbank als neuer Zustand gespeichert wer-

den, ist es weder möglich, sich mit einer zuvor erfolgten Kopie, die noch den vorherigen Stand wiedergibt, anzumelden, noch ist es möglich, den neuen Stand auf der sich verändernden Datenbank zu kopieren, da er nicht statisch bleibt, sondern sich kontinuierlich weiterverändert, *vgl. Beschreibungsseiten 5 und 6.*

Damit stellt die spezielle Zusammensetzung des Schlüssels, bei dem zwischen zwei Authentifizierungszeitpunkten die lokal veränderbaren Zeichen nur in der Kommunikationseinrichtung, nicht jedoch in der zentralen Datenbank und die zentral veränderbaren Zeichen oder Zeichenfolge nur in der zentralen Datenbank, aber nicht in der Kommunikationseinrichtung veränderbar sind, ein die Sicherheit des Schlüssels erhöhendes technisches Merkmal dar.

Dieses Merkmal ist im Hinblick auf die Frage einer erfinderischen Tätigkeit gemäß § 4 PatG uneingeschränkt zu prüfen.

Da die Prüfungsstelle diesbezüglich keine Recherche durchgeführt hat, ist der relevante Stand der Technik noch zu recherchieren.

6. Bei dieser Sachlage war der Beschluss der Prüfungsstelle für Klasse H04L vom 11. Januar 2016 aufzuheben und die Anmeldung zur weiteren Prüfung an das Deutsche Patent- und Markenamt zurückzuverweisen.

III.

R e c h t s m i t t e l b e l e h r u n g

Gegen diesen Beschluss steht dem Anmelder - vorbehaltlich des Vorliegens der weiteren Rechtsmittelvoraussetzungen, insbesondere einer Beschwer - das Rechtsmittel der Rechtsbeschwerde zu. Da der Senat die Rechtsbeschwerde nicht

zugelassen hat, ist sie nur statthaft, wenn einer der nachfolgenden Verfahrensmängel gerügt wird, nämlich

1. dass das beschließende Gericht nicht vorschriftsmäßig besetzt war,
2. dass bei dem Beschluss ein Richter mitgewirkt hat, der von der Ausübung des Richteramtes kraft Gesetzes ausgeschlossen oder wegen Besorgnis der Befangenheit mit Erfolg abgelehnt war,
3. dass einem Beteiligten das rechtliche Gehör versagt war,
4. dass ein Beteiligter im Verfahren nicht nach Vorschrift des Gesetzes vertreten war, sofern er nicht der Führung des Verfahrens ausdrücklich oder stillschweigend zugestimmt hat,
5. dass der Beschluss aufgrund einer mündlichen Verhandlung ergangen ist, bei der die Vorschriften über die Öffentlichkeit des Verfahrens verletzt worden sind, oder
6. dass der Beschluss nicht mit Gründen versehen ist.

Die Rechtsbeschwerde ist **innerhalb eines Monats** nach Zustellung des Beschlusses

schriftlich durch einen beim Bundesgerichtshof zugelassenen Rechtsanwalt als Bevollmächtigten beim Bundesgerichtshof, Herrenstr. 45 a, 76133 Karlsruhe, einzureichen oder

durch einen beim Bundesgerichtshof zugelassenen Rechtsanwalt als Bevollmächtigten in elektronischer Form bei der elektronischen Poststelle des BGH, www.bundesgerichtshof.de/erv.html. Das elektronische Dokument ist mit einer prüfbaren qualifizierten elektronischen Signatur nach dem Signaturgesetz oder mit einer prüfbaren fortgeschrittenen elektronischen Signatur zu versehen. Die Eignungsvoraussetzungen für eine Prüfung und für die Formate des elektronischen

Dokuments werden auf der Internetseite des Bundesgerichtshofs www.bundesgerichtshof.de/erv.html bekannt gegeben.

Dr. Strößner Brandt Dr. Friedrich Dr. Himmelmann

prö