BUNDESPATENTGERICHT

18 W (pat) 50/14

_____

(Aktenzeichen)

Verkündet am
19. November 2014
…

B E S C H L U S S

In der Beschwerdesache

betreffend die Patentanmeldung 101 95 999.0-53

…

hat der 18. Senat (Technischer Beschwerdesenat) des Bundespatentgerichts auf die mündliche Verhandlung vom 19. November 2014 durch die Vorsitzende Richterin Dipl.-Ing. Wickborn sowie die Richter Kruppa, Dipl.-Phys. Dr. Schwengelbeck und die Richterin Dipl.-Phys. Dr. Otten-Dünnweber

beschlossen:

1. Der Beschluss der Prüfungsstelle für Klasse G 06 F des Deutschen Patent- und Markenamts vom 3. Juni 2009 wird aufgehoben.
2. Die Sache wird zur Entscheidung an das Deutsche Patent- und Markenamt zurückverwiesen.

G r ü n d e

I.

Die vorliegende Patentanmeldung 101 95 999.0 geht hervor aus einer PCT-Anmeldung (Veröffentlichungsnummer WO 01/75595 A2) und ist am 14. März 2001 unter Inanspruchnahme einer US-amerikanischen Priorität vom 31. März 2000 eingereicht worden. Sie trägt in der deutschen Übersetzung die Bezeichnung

„Kontrollieren von Zugriffen auf isolierten Speicher unter Verwendung einer Speichersteuereinrichtung für eine isolierte Ausführung“.

Die Anmeldung wurde durch die Prüfungsstelle für Klasse G 06 F des Deutschen Patent- und Markenamts mit Beschluss vom 3. Juni 2009 zurückgewiesen, weil der Gegenstand des (damals geltenden) Anspruchs 1 im Hinblick auf die im Prüfungsverfahren ermittelten Druckschriften

D4: **SMITH, S. W., WEINGART, S.: Building a high-performance, programmable secure coprocessor. In: Computer Networks 31, 1999, Seiten 831 – 860** und

D5: **US 5 912 453 A**

nicht auf einer erfinderischen Tätigkeit beruhe.

Gegen diesen Beschluss richtet sich die Beschwerde der Anmelderin.

Im Prüfungsverfahren sind ferner die folgenden Druckschriften genannt worden:

D1: **US 5 522 075 A**

D2: **US 5 628 023 A**

D3: **ARBAUGH, W. A. u. a.: A Secure and Reliable Bootstrap Architecture. In: IEEE Symposium on Security and Privacy, 4. – 7. Mai 1997, Proceedings, ISBN: 0-8186-7828-3, Seiten 65 – 71.**

Die Beschwerdeführerin beantragt,

den Beschluss der Prüfungsstelle für Klasse G 06 F des Deutschen Patent- und Markenamts vom 3. Juni 2009 aufzuheben und das Patent auf der Grundlage der folgenden Unterlagen zu erteilen:

- Patentansprüche 1 - 7, eingereicht in der mündlichen Verhandlung,
- Beschreibung Seiten 1 - 33,
- Figuren 1A - 1C, 2A, 2B, 3A, 3B, 4 - 9, jeweils eingegangen am 30. September 2002.

Der seitens des Senats mit einer Gliederung versehene geltende Patentanspruch 1 lautet:

„Computersystem (100) mit

Ma (a) wenigstens einem Prozessor (110), der in einem normalen und in einem isolierten Ausführungsmodus betrieben werden kann, wobei der Inhalt eines Prozessorsteuerregisters (252) anzeigt, ob sich der Prozessor (110) in dem isolierten Ausführungsmodus befindet,

Mb (b) einem Systemspeicher (140) mit einem isolierten physikalischen Speicherbereich (70), auf den der Prozessor (110) nur in dem isolierten Ausführungsmodus zugreifen kann, und

Mc (c) einem mit dem Prozessor (110) und dem Systemspeicher (140) gekoppelten Chipsatz (130, 150, 160), der eine mit dem Systemspeicher (140) gekoppelte Zugriffssteuereinrichtung (135) enthält,

Md wobei der isolierte Ausführungsmodus durch Ausführung eines privilegierten Befehls (iso_init) in dem Prozessor (110) initialisiert wird, der einen Prozessor-Nub-Lader (52) aufruft und in den isolierten Speicherbereich (70) lädt, wobei der Prozessor-Nub-Lader (52) ein in dem Chipsatz (130, 150, 160) gehaltener geschützter Bootstrap-Lader-Code ist, der ein Prozessor-Nub-Softwaremodul (18) in den isolierten Speicherbereich (70) lädt und dessen Integrität überprüft, wobei das Prozessor-Nub-Softwaremodul (18) hardwarebezogene Dienste für die isolierte Ausführung zur Verfügung stellt,

wobei die Zugriffssteuereinrichtung (135) aufweist:

Mc1 (c1) einen von dem Prozessor (110) konfigurierbaren Konfigurationsspeicher (610), der eine den isolierten physikalischen Speicherbereich (70) definierende Konfigurationseinstellung (612) in Speicherbereichsregistern (620, 630) speichert,

Mc2 (c2) einen Zugriffsgewährungsgenerator (650), der bei einer Zugriffstransaktion von dem Prozessor (110) Zugriffsinformationen (660) empfängt, die eine physikalische Adresse (662) und ein Isolierter-Zugriff-Signal (664) umfassen, wobei das Isolierter-Zugriff-Signal (664) angelegt wird, wenn der Prozessor (110) eine gültige Referenz auf den isolierten Speicherbereich (70) erzeugt, wobei der Zugriffsgewährungsgenerator (650) aus dem Konfigurationsspeicher (610) die Konfigurationseinstellung (612) empfängt und aus dieser und den Zugriffsinformationen (660; 662, 664) ein Zugriffsgewährungssignal (652) erzeugt, wenn die physikalische Adresse außerhalb des isolierten Speicherbereichs (70) liegt oder wenn die physikalische Adresse (662) innerhalb des isolierten Speicherbereichs (70) liegt und das Isolierter-Zugriff-Signal (664) eine gültige Referenz auf den isolierten Speicherbereich (70) anzeigt, wobei andernfalls von der Zugriffssteuereinrichtung (135) anstelle des Inhalts des isolierten Speicherbereichs (70) ein vorgegebener Datenwert zurückgegeben wird, und

Mc3 (c3) eine Konfigurationssteuereinrichtung (640) zum Steuern des Zugriffs auf die Speicherbereichsregister (620, 630) des Konfigurationsspeichers (610) mit

einem Steuerspeicher (710) zum Speichern eines Verriegelungssteuerworts (712), wobei das Verriegelungssteuerwort (712) anzeigt, ob der isolierte Speicherbereich (70) freigegeben ist, und durch das Prozessor-Nub-Softwaremodul (18) geschrieben wird, wenn dieses aufgerufen wird, um den isolierten Speicherbereich (70) zu initialisieren, und

einen Verriegler (720) zum Sperren des Zugriffs auf die Speicherbereichsregister (620, 630) des Konfigurationsspeichers (610) auf der Grundlage des Verriegelungssteuerworts (712).“

Wegen der geltenden abhängigen Ansprüche 2 bis 7 wird auf den Akteninhalt verwiesen.

Die Beschwerdeführerin macht hierzu geltend, dass die geänderte Anspruchsfassung zulässig sei und die Gegenstände der Ansprüche neu und erfinderisch seien.

Wegen der weiteren Einzelheiten wird auf den Akteninhalt verwiesen.

II.

Die zulässige Beschwerde führt zur Aufhebung des angefochtenen Beschlusses und zur Zurückverweisung der Sache an das Deutsche Patent- und Markenamt gemäß § 79 Abs. 3 Satz 1 Nr. 1 und Nr. 3 PatG.

1. Die Patentanmeldung betrifft die Sicherheit von Mikroprozessoren. Moderne Mikroprozessorsysteme stellten den Benutzern bequeme und effiziente Verfahren zur Ausführung von Geschäften, zur Kommunikation und Transaktion zur Verfügung, seien aber auch anfällig für skrupellose Angriffe, wie Viren. Die vorhandenen Techniken zum Schutz gegen Angriffe wiesen Nachteile auf. Antivirenprogramme könnten nur bekannte Viren erfassen und verwendeten meist eine schwache Vorgehensweise, bei der eine Datei als gut gelte, solange sie sich nicht als schlecht herausgestellt habe. Diese Vorgehensweise könnte für viele Sicherheitsanwendungen nicht ausreichend sein (vgl. Beschreibung, S. 1, Z. 9 – S. 2, Z. 12).

Die der Anmeldung zugrunde liegende **Aufgabe** besteht sinngemäß darin, die Sicherheit in einem Computersystem zu erhöhen, unabhängig von ggf. in dem Be-

triebssystem und dem Prozessor vorliegenden verschiedenen Hiercharchieebenen bzw. Privilegniveaus (vgl. Beschreibung S. 4, Z. 18 – S. 5, Z. 8).

Die der Erfindung zugrunde liegende **objektive Aufgabe** besteht darin, bei einem Prozessor, der in einem normalen und einem isolierten Ausführungsmodus betrieben werden kann, sicherzustellen, dass auf einen vorgesehenen isolierten Speicherbereich ausschließlich autorisierte Zugriffe zugelassen werden.

Als **Fachmann** zur Lösung dieser Aufgabe sieht der Senat einen Ingenieur der Informationstechnik (FH) an, der über Berufserfahrung in der Konzeption von sicheren Computersystemen verfügt.

Die Aufgabe soll gelöst werden durch ein Computersystem nach Anspruch 1, bei dem der isolierte Ausführungsmodus durch einen privilegierten Befehl in dem Prozessor initialisiert wird und der Zugriff auf den isolierten Speicherbereich nur freigegeben wird, wenn die von dem Prozessor bei einer Zugriffstransaktion erzeugten Zugriffsinformationen den festgelegten Konfigurationseinstellungen entsprechen. Ein Verriegler soll den Zugriff auf den Konfigurationsspeicher auf der Grundlage eines Verriegelungssteuerwortes sperren.

2. Einige Merkmale des Patentanspruchs 1 bedürfen der Auslegung.

Patentanspruch 1 ist auf ein Computersystem gerichtet, das mit einem Prozessor, einem Systemspeicher mit einem isolierten physikalischen Speicherbereich, einem Chipsatz und einer Zugriffssteuereinrichtung mit einem Zugriffsgewährungsgenerator und einem Konfigurationsspeicher mit Konfigurationssteuereinrichtung ausgestattet ist (Merkmale Ma, Mb, Mc, Mc1, Mc2, Mc3). Der Prozessor kann in zwei verschiedenen Ausführungsmodi betrieben werden, einem normalen Ausführungsmodus und einem isolierten Ausführungsmodus: Der normale Ausführungsmodus stellt dabei einen Modus dar, in welchem der Prozessor in einer nicht sicheren Umgebung oder einer normalen Umgebung ohne die von dem isolierten

Ausführungsmodus zur Verfügung gestellten Sicherheitsmerkmale betrieben wird (vgl. Beschreibung, S. 10, Z. 3 – 7). Der Systemspeicher enthält einen isolierten Speicherbereich und einen nicht-isolierten Bereich (vgl. Beschreibung, S. 8, Z. 4 – 5). Auf den isolierten physikalischen Speicherbereich des Systemspeichers kann der Prozessor nur zugreifen, wenn er sich in dem isolierten Ausführungsmodus befindet (Merkmale Ma, Mb). Der isolierte Ausführungsmodus wird durch Ausführung eines privilegierten Befehls initialisiert, der einen Prozessor-Nub-Lader, d. h. einen Lader-Code, in den isolierten Speicherbereich lädt, welcher wiederum ein Prozessor-Nub-Softwaremodul in den isolierten Speicherbereich lädt und auf Integrität überprüft (Merkmal Md). Dabei stellt das Prozessor-Nub-Softwaremodul hardwarebezogene Dienste für die isolierte Ausführung zur Verfügung, etwa indem es den Betriebssystem-Nub überprüft und lädt sowie beispielsweise eine Schlüsselverwaltung und Schnittstellenabstraktionen zur Verfügung stellt (vgl. Beschreibung, S. 6, Z. 34 – S. 7, Z. 3 sowie S. 15, Z. 10 – 22). Bei einem Computersystem, das – wie aus dem Stand der Technik bekannt – verschiedene Hierarchieebenen, d. h. verschiedene als Ringe bezeichnete Privilegierungsstufen aufweist, soll jeder dieser Privilegierungsringe in dem isolierten oder dem normalen Ausführungsmodus betrieben werden können (vgl. Beschreibung, S. 4, Z. 18 – S. 5, Z. 21).

Welche Adressbereiche im Systemspeicher den isolierten physikalischen Speicher darstellen, ist durch die den isolierten Speicherbereich definierende Konfigurationseinstellung im Konfigurationsspeicher festgelegt (Merkmale Mc1, Mc2, vgl. auch S. 31, Z. 24 – 28 der Beschreibung). Ein Isolierter-Zugriff-Signal wird nur dann angelegt, wenn der Prozessor, der in dem isolierten Ausführungsmodus betrieben wird, eine gültige Referenz auf den isolierten Speicherbereich erzeugt. Der Zugriffsgewährungsgenerator gibt für Adressen außerhalb des isolierten Speicherbereichs den Zugriff uneingeschränkt frei, für Adressen innerhalb des isolierten Speicherbereichs den Zugriff jedoch nur, wenn sich der Prozessor im isolierten Ausführungsmodus befindet (vgl. Merkmal Mc2).

Der Prozessor kann die Konfigurationseinstellung im Konfigurationsspeicher konfigurieren; der Zugriff auf den Konfigurationsspeicher wird dabei durch eine Konfigurationssteuereinrichtung gesteuert, die den Zugriff in Abhängigkeit eines Verriegelungssteuerworts sperrt (vgl. Merkmale Mc1 und Mc3).

3. Die Patentansprüche sind zulässig.

Die Merkmale der geltenden Ansprüche sind durch die ursprünglichen Patentansprüche sowie die ursprünglich eingereichte Beschreibung mit den Figuren 1A bis 9 als zur Erfindung gehörig offenbart:

Patentanspruch 1 basiert auf den ursprünglichen Ansprüchen 31, 34 und 35, den Figuren 1A, 1B, 1C, 2B, 6, 7 und 8 i. V. m. der ursprünglichen Beschreibung Seite 6, Zeilen 3 bis 7, 14 bis 18 und 27 bis 33, Seite 8, Zeilen 4 und 5, Seite 9, Zeilen 4 bis 19, Seite 10, Zeilen 18 bis 24, Seite 11, Zeile 35 bis Seite 12, Zeile 6, Seite 13, Zeile 31 bis Seite 14, Zeile 5, Seite 20, Zeilen 7 bis 13, Seite 25, Zeile 34 bis Seite 26, Zeile 1, Seite 27, Zeilen 5 bis 16, 18 bis 21 und 26 bis 31, Seite 28, Zeilen 3 bis 9 und 20 bis 25, Seite 31, Zeilen 11 bis 19 sowie Seite 32, Zeilen 10 bis 27.

Die Merkmale der auf den Anspruch 1 direkt oder indirekt rückbezogenen Unteransprüche sind wie folgt offenbart: Anspruch 2 ist offenbart durch den ursprünglichen Anspruch 37 i. V. m. Figur 7 und Seite 30, zweiter Absatz, Anspruch 3 durch Seite 13, Zeilen 17 bis 23, Anspruch 4 durch Seite 6, Zeile 34 bis Seite 7, Zeile 10 i. V. m. Figur 1A und Seite 4, Zeile 18 bis Seite 5, Zeile 21, Anspruch 5 durch Seite 26, Zeilen 14 - 16 und 33 bis 35, Figur 1C und Seite 11, Zeilen 30 und 31, Anspruch 6 durch die ursprünglichen Ansprüche 33 und 38 bis 40 i. V. m. Figur 8

und Seite 30, Zeile 22 bis Seite 31, Zeile 6 und Seite 31, Zeilen 11 bis 15, sowie Anspruch 7 durch die Figuren 2A, 2B, 3A und 6 i. V. m. Seite 17, Zeilen 13 bis 18, Seite 19, Zeilen 14 bis 16, Seite 20, Zeilen 4 bis 18, Seite 21, Zeilen 6 bis 32 und Seite 26, Zeilen 16 bis 19.

4. Der im bisherigen Prüfungsverfahren genannte Stand der Technik steht dem geltenden Patentanspruch 1 nicht patenthindernd entgegen, da er dem Fachmann keine Anregung gibt, ein Computersystem mit sämtlichen in Anspruch 1 aufgeführten Merkmalen auszugestalten.

a) Der Gegenstand des Anspruchs 1 ist neu gegenüber dem im Verfahren befindlichen Stand der Technik.

Druckschrift **D1** beschreibt für ein Computersystem, das mit mehreren hierarchisch angeordneten Privilegringen ausgestattet ist, die Regulierung des Speicherzugriffs (vgl. Fig. 7B und Sp. 1, Z. 54 – 58). Je nach Privilegmodus kann auf unterschiedliche Speicherbereiche zugegriffen werden (vgl. Sp. 5, Abschnitt 1.5.2 *Memory Access*). Die Druckschrift gibt keinen Hinweis auf einen isolierten Ausführungsmodus im Sinne der Merkmale Ma, Mb und Md, der durch Ausführung eines privilegierten Befehls initialisiert wird, oder auf einen Konfigurationsspeicher und eine Konfigurationssteuereinrichtung gemäß den Merkmalen Mc1, Mc2 und Mc3.

Druckschrift **D2** offenbart einen Computer mit einem virtuellen Speicher, über den ein geschützter Zugriff auf einen realen Speicher des Computersystems zur Verfügung gestellt wird (vgl. Abstract). Einem Programm wird der Zugriff auf die gesicherten Seiten des Speichers erlaubt, wenn es sich durch ein entsprechendes *Token* ausweisen kann (vgl. Sp. 6, Z. 1 – 20). Die Druckschrift beschreibt dabei einen mit einem Prozessor *100* und einem Systemspeicher (*main memory 110*)

gekoppelten Chipsatz (*protection verification facility 105*), der eine mit dem Systemspeicher gekoppelte Zugriffssteuereinrichtung enthält (vgl. Fig. 1 und Sp. 8, Z. 1 – 52: *address translation and protection verification facility* / Merkmal **Mc**). Der in Druckschrift D2 beschriebene Verifizierungsablauf (*protection verification process 140*) stellt dabei einen Zugriffsgewährungsgenerator dar, der von dem Prozessor Zugriffsinformationen empfängt, die eine – allerdings virtuelle – Adresse (*virtual address 130*) und ein Isolierter-Zugriff-Signal umfassen (*token 125,* vgl. Fig. 1 mit zugehöriger Beschreibung). In Abhängigkeit von der für den angeforderten Seitenrahmen gesetzten Konfigurationseinstellung (vgl. Fig. 3: *step 555: page protected?*) und der vom Prozessor gelieferten Zugriffsinformation wird der Zugriff auf die Seite gewährt oder nicht gewährt (vgl. Sp. 19, Z. 41 – Sp. 20, Z. 6). Dabei wird ein Zugriffsgewährungssignal erzeugt, dass den Zugriff erlaubt oder nicht erlaubt. Dieser Verifizierungsablauf stimmt mit dem in Merkmal **Mc2** geforderten Zugriffsgewährungsgenerator **teilweise** überein, die Zugriffsgewährung erfolgt aber über ein Token anstatt, wie in der vorliegenden Patentanmeldung beansprucht, über einen reinen Adressvergleich. Druckschrift D2 gibt keinen Hinweis darauf, einen Prozessor im Sinne der Merkmale Ma, Mb und Md in einem normalen und einem isolierten Ausführungsmodus zu betreiben oder den Systemspeicher mit einem isolierten physikalischen Speicherbereich gemäß Merkmal Mb auszustatten; ebenso fehlen Hinweise auf einen konfigurierbaren Konfigurationsspeicher und eine Konfigurationssteuereinrichtung gemäß den Merkmalen Mc1 und Mc3.

Druckschrift **D3** beschreibt einen speziellen Bootprozess (*AEGIS*), bei dem der gesamte ausführbare Code vor der Ausführung über eine digitale Signatur verifiziert wird (vgl. S. 66 - 67, Abschnitt 3.1 *Overview*). Angaben zu einem anspruchsgemäßen Konfigurationsspeicher, einem Zugriffsgewährungsgenerator oder einem in zwei verschiedenen Modi betreibbaren Prozessor sind der Druckschrift nicht zu entnehmen.

Druckschrift **D4** offenbart einen sicheren Coprozessor (*secure coprocessor / 486 Processor*), für den eine mehrschichtige Software-Architektur bereitgestellt wird (vgl. Titel, Fig. 1 und 3 sowie S. 833, Abschnitt *1.3.4 Software design*). Der Coprozessor verfügt über verschiedene Ausführungsmodi, wobei ein in einem Register gespeicherter Sperrwert (*ratchet = 0* bzw. *1, 2, 3, 4*) anzeigt, in welchem Modus der Coprozessor sich befindet (vgl. Fig. 8 und S. 844, re. Sp., le. Abs., zw. Satz / **teilweise** Merkmal **Ma**, ohne Angabe eines isolierten und eines normalen Ausführungsmodus). Der Systemspeicher (*BBRAM*, Fig. 1) weist geschützte Bereiche auf, wobei eine Hardware-Verriegelung den Zugriff auf diese Bereiche erlaubt oder versagt (vgl. S. 845, re. Sp., Abschnitt 6.4), so dass der Coprozessor in den verschiedenen Ausführungsmodi nur auf den jeweils zugeordneten physikalischen Speicherbereich zugreifen kann (**teilweise** Merkmal **Mb**, ohne Angabe eines isolierten Ausführungsmodus). Diese Hardware-Verriegelung (*hardware Locks*) stellt eine mit dem Systemspeicher (*BBRAM)* gekoppelte Zugriffssteuereinrichtung gemäß Merkmal **Mc** dar, welche Teil eines mit dem Prozessor (*486 processor*) und dem Systemspeicher gekoppelten Chipsatzes ist (vgl. Fig. 1, Speicher *FLASH, ROM; Routing Control,* S. 832, Abschnitt *1.3.1 Hardware design*).

Die in Druckschrift D4 offenbarte Hardware-Verriegelung arbeitet als ein Zugriffsgewährungs-Generator (vgl. S. 845, li. Sp. erster Satz), der bei einer Zugriffstransaktion von dem Prozessor als Zugriffsinformation zwangsläufig sowohl den die Funktion eines Isolierter-Zugriff-Signal übernehmenden Sperrwert empfangen muss als auch die Seite im Speicher, auf die zugegriffen werden soll (vgl. Table 1 und S. 845, Abschnitt 6.4, dr. Satz), welche eine physikalische Adresse darstellt (Merkmal **Mc2**). Der Fachmann liest dabei mit, dass eine Art Zugriffsgewährungssignal erzeugt wird, wenn die bei der Zugriffstransaktion angeforderte Adresse innerhalb des geschützten Speicherbereichs (z.B. *Protected page 1)* liegt und der Sperrwert (z.B. *ratchet 1*) den zugehörigen Modus anzeigt (**teilweise** Merkmal **Mc2**, ohne dass eine aus einem Konfigurationsspeicher empfangene Konfigurationseinstellung und ein Isolierter-Zugriff-Signal aufgeführt sind).

Druckschrift D4 gibt keinen Hinweis auf einen isolierten Ausführungsmodus, welcher durch Ausführung eines privilegierten Befehls initialisiert werden kann, der

einen Lader-Code gemäß Merkmal Md aufruft. Auch zu einem Konfigurationsspeicher oder einer Konfigurationssteuereinrichtung mit einem Steuerspeicher und einem Verriegler ist der Druckschrift nichts zu entnehmen (Merkmale Mc1, Mc3, Mc3.1, Mc3.2 fehlen). Gegeben wird lediglich der allgemeinere Hinweis, dass aus Sicherheitsgründen bei Feststellen eines Manipulationsversuchs der gesamte Systemspeicher zu initialisieren ist (vgl. S. 839, li. Sp., zw. Abs., zw. Satz).

Druckschrift **D5** betrifft die Integration verschiedener Anwendungsprogramme auf einer Chipkarte, auf der ein Prozessor und eine Speichereinheit angeordnet sind (vgl. Fig. 2 und 3: *common processor area 110, common memory 100*). Die Druckschrift geht von einem Speicher aus, der in einen geschützten Bereich, auf den z. B. das Betriebssystem zugreifen kann, und einen ungeschützten Bereich, auf den die Anwendungsprogramme zugreifen können, aufgeteilt ist (vgl. Sp. 2, Z. 57 – 67). Dabei wird den verschiedenen Anwendungsprogrammen jeweils nur Zugriff auf den ihnen jeweils – dynamisch – zugeordneten Speicherbereich gewährt (vgl. Sp. 4, Z. 5 – 16: *specified area*, *predetermined memory area*), was durch Applikationstabellen oder durch spezielle Registerbits gesteuert werden kann (vgl. Sp. 5, Z. 7 – 42). Zusätzlich sollen die Anwendungsprogramme aber auch Zugriff auf Speicherbereiche haben, die allgemein zugängliche Daten des Betriebssystems enthalten (Sp. 4, Z. 12 – 16). Damit stellt der dem jeweiligen Anwendungsprogramm zugeordnete Speicherbereich einen isolierten physikalischen Speicherbereich dar (**teilweise** Merkmal **Mb**), eine Unterteilung in einen isolierten und einen normalen Ausführungsmodus gemäß den Merkmalen Ma und Md als nicht gleichrangige Ausführungsmodi des Prozessors ist damit jedoch nicht gegeben.
Druckschrift D5 offenbart eine mit dem Systemspeicher *100* gekoppelte Zugriffssteuereinrichtung (vgl. Blöcke *200* – *240* im gestrichelt umrandeten linken Block der Fig. 2 / Merkmal **Mc**). Dabei stellt die Anwendungstabelle (*application table 230*) einen Konfigurationsspeicher im Sinne des Merkmals **Mc1** dar, da in ihr die den jeweiligen Anwendungsprogrammen zugeordneten Anfangs- und Endadressen abgelegt sind, welche den „isolierten“ physikalischen Speicherbereich definie-

ren (vgl. Sp. 7, Z. 21 – 66 und Anspruch 1, erster Abs. in Sp. 10). Die aus einem Adress-Komparator (*address comparator 220*) und einem Interrupt-Decodier-Schaltkreis (*interruption-decoding logic circuit 240*) bestehende Kombination fungiert somit als ein Zugriffsgewährungsgenerator, der von dem Prozessor Zugriffsinformationen empfängt (vgl. Fig. 2 und Sp. 7, Z. 21 – 29). Der Fachmann liest dabei mit, dass diese Zugriffsinformationen eine physikalische Adresse umfassen (vgl. Sp. 7, insbes. Z. 46, 47: *addresses filed on the address bus*), ein Hinweis auf ein Isolierter-Zugriff-Signal im Sinne der Anmeldung ist Druckschrift D5 jedoch nicht zu entnehmen. Für die alternative Ausgestaltung mit einem Decoder anstelle des Adress-Komparators wird beschrieben (vgl. Sp. 8, Z. 17 – 20, Anspruch 1, le. Abs.), dass dieser die Adressregion, welche durch das Anfangs- und Endregister definiert ist, autorisiert, was bedeutet, dass der Zugriff gewährt wird, wenn die physikalische Adresse innerhalb des „isolierten“ Speicherbereichs liegt. Zusätzlich ist der Zugriff auf allgemeine Speicherbereiche auch erlaubt (vgl. Sp. 6, Z. 3 – 8), was bedeutet, dass der Zugriff auf Speicherbereiche außerhalb des „isolierten“ Speicherbereichs ebenfalls gewährt wird. Hinsichtlich der Gewährung eines Zugriffs dürfte der Fachmann mitlesen, dass hierzu ein Zugriffsgewährungssignal erzeugt wird, so dass aus Druckschrift D5 für den Fachmann **teilweise** das Merkmal **Mc2** nahegelegt ist (ohne Angabe eines Isolierter-Zugriff-Signals).

Der Fachmann entnimmt Druckschrift D5 auch eine Konfigurationssteuereinrichtung, die Zugriffe auf den Konfigurationsspeicher (*application table*) steuert, wobei die Festlegung der Adressbereiche der jeweiligen Speicherbereiche durch das Betriebssystem vorgenommen wird und eine nachträgliche Änderung dieser Adressbereiche verunmöglicht werden soll (vgl. Sp. 8, Z. 13 – 16 und Sp. 5, Z. 7 – 26 / Merkmal **Mc3**). Die Adressbereiche in der Applikationstabelle werden durch das Betriebssystem beim Laden des Anwendungsprogramms festgelegt, was dem Schreiben eines Verriegelungssteuerwortes in einen Steuerspeicher durch ein Prozessor-Nub-Softwaremodul entspricht (**teilweise** Merkmal **Mc3.1**, ohne die Angabe, dass dies bei Aufruf des Prozessor-Nub-Softwaremoduls, d. h. bei Initialisierung eines isolierten Ausführungsmodus erfolgt). Dabei entspricht die Angabe,

dass eine Manipulation nicht möglich sein soll, dem in Merkmal **Mc3.2** geforderten Sperren des Zugriffs (vgl. Sp. 7, Z. 61 – Sp. 8, Z. 8; Sp. 5, Z. 12 – 16).

Somit offenbart keine der im Verfahren befindlichen Schriften ein Computersystem mit sämtlichen Merkmalen des Gegenstands des geltenden Patentanspruchs 1.

b) Der Gegenstand des Anspruchs 1 ist dem Fachmann durch den im Verfahren befindlichen Stand der Technik auch nicht nahegelegt.

Ein Prozessor, der in einem normalen und in einem isolierten Ausführungsmodus im Sinne der Merkmale Ma, Mb und Md betrieben werden kann, ist aus den Druckschriften D1 bis D5 nicht bekannt.

Druckschrift D5 offenbart dabei lediglich einen vom Prozessor konfigurierbaren Konfigurationsspeicher, über den die Speicherbereiche, welche verschiedenen – gleichrangigen – Anwendungsprogrammen zugeordnet werden, definiert werden. Weder Druckschrift D5 noch der weitere im Verfahren befindliche Stand der Technik gibt dem Fachmann eine Anregung, einen einstellbaren Konfigurationsspeicher auch für Speicherbereiche eines Systemspeichers zu implementieren, die nicht den Anwendungsprogrammen zugeordnet sind.

Für den Fachmann ist ein Computersystem gemäß Anspruch 1 daher auch durch eine beliebige Zusammenschau der Druckschriften D1 bis D5 nicht nahegelegt.

Auch das allgemeine Fachwissen gibt dem Fachmann keine Anregungen, für einen Prozessor einen normalen und einen isolierten Ausführungsmodus zu implementieren, wobei der isolierte Ausführungsmodus durch einen privilegierten Befehl initialisiert wird und wobei der Prozessor den Speicherbereich, auf den nur im isolierten Modus zugegriffen werden kann, über eine in einem Konfigurationsspeicher gespeicherte Konfigurationseinstellung konfigurieren kann.

Der beanspruchte Gegenstand geht somit über das übliche fachmännische Handeln, ausgehend von den Lehren der betrachteten Druckschriften D1 bis D5 und unter Einbeziehung des Fachwissens hinaus.

Damit trägt der im Zurückweisungsbeschluss genannte Grund nicht mehr.

5. Einige der in den geltenden Patentanspruch 1 neu aufgenommenen Merkmale entstammen der Beschreibung sind ersichtlich nicht Gegenstand der Recherche im bisherigen Prüfungsverfahren gewesen.

Der Senat hat daher nach § 79 Abs. 3 Satz 1 Nr. 1 und Nr. 3 PatG davon abgesehen, in der Sache selbst zu entscheiden und das Patent zu erteilen, weil er die Frage, ob der Gegenstand des geltenden Patentanspruchs 1 auch auf einer erfinderischen Tätigkeit beruht, anhand des derzeit ermittelten Standes der Technik nicht abschließend beurteilen kann.

Denn die beanspruchten detaillierten Merkmale des Computersystems hinsichtlich eines isolierten Ausführungsmodus eines Prozessors, welcher durch Ausführung eines privilegierten Befehls initialisiert wird, wobei der Prozessor die den isolierten Speicherbereich definierende, in einem Konfigurationsspeicher gespeicherte Konfigurationseinstellung konfigurieren kann, sind im bisherigen Verfahren noch nicht recherchiert worden, da im Prüfungsverfahren verschiedene Ausführungsmodi eines Prozessors allein im Zusammenhang mit verschiedenen hierarchischen Privilegniveaus diskutiert worden sind.

Es kann daher nicht ausgeschlossen werden, dass insbesondere unter dem Gesichtspunkt der §§ 3 und 4 PatG ein einer Patenterteilung möglicherweise entgegenstehender Stand der Technik existiert. Zu deren Ermittlung sind in erster Linie die Prüfungsstellen des Patentamts berufen, welche hierzu über geeignete Re-

cherchemittel und Fachkenntnisse verfügen. Da eine sachgerechte Entscheidung nur aufgrund einer vollständigen Recherche des relevanten Standes der Technik ergehen kann, war die Sache – auch um der Anmelderin keine Tatsacheninstanz zu nehmen – zur weiteren Prüfung und Entscheidung an das Deutsche Patent- und Markenamt zurückzuverweisen (§ 79 Abs. 3 Satz 1 Nr. 1 und Nr. 3 PatG).

III.

Rechtsmittelbelehrung

Gegen diesen Beschluss steht den am Beschwerdeverfahren Beteiligten das Rechtsmittel der Rechtsbeschwerde zu. Da der Senat die Rechtsbeschwerde nicht zugelassen hat, ist sie nur statthaft, wenn gerügt wird, dass

1. das beschließende Gericht nicht vorschriftsmäßig besetzt war,
2. 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. einem Beteiligten das rechtliche Gehör versagt war,
4. ein Beteiligter im Verfahren nicht nach Vorschrift des Gesetzes vertreten war, sofern er nicht der Führung des Verfahrens ausdrücklich oder stillschweigend zugestimmt hat,
5. der Beschluss aufgrund einer mündlichen Verhandlung ergangen ist, bei der die Vorschriften über die Öffentlichkeit des Verfahrens verletzt worden sind, oder
6. der Beschluss nicht mit Gründen versehen ist.

Die Rechtsbeschwerde ist innerhalb eines Monats nach Zustellung des Beschlusses beim Bundesgerichtshof, Herrenstr. 45 a, 76133 Karlsruhe, durch einen beim Bundesgerichtshof zugelassenen Rechtsanwalt als Bevollmächtigten schriftlich einzulegen.

Wickborn Kruppa Dr. Schwengelbeck Dr. Otten-Dünnweber

Hu