Interner Verteilerschlüssel:

(A) [-] Veröffentlichung im ABl.
(B) [-] An Vorsitzende und Mitglieder
(C) [-] An Vorsitzende
(D) [X] Keine Verteilung

Datenblatt zur Entscheidung vom 21. Juni 2017

Beschwerde-Aktenzeichen: T 2291/12 - 3.4.03

Anmeldenummer: 99924992.3

Veröffentlichungsnummer: 1080454

IPC: G07F7/10, G06F1/00

Verfahrenssprache: DE

Bezeichnung der Erfindung:
ZUGRIFFSGESCHÜTZTER DATENTRÄGER

Anmelder:
Giesecke & Devrient GmbH

Stichwort:

Relevante Rechtsnormen:
EPÜ Art. 54(3)
EPÜ 1973 Art. 54(1), 54(2), 56, 82, 87

Schlagwort:
Neuheit - (ja)
Erfinderische Tätigkeit - (ja)

Zitierte Entscheidungen:

Orientierungssatz:

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

European Patent Office
D-80298 MUNICH
GERMANY
Tel. +49 (0) 89 2399-0
Fax +49 (0) 89 2399-4465

Beschwerde-Aktenzeichen: T 2291/12 - 3.4.03

E N T S C H E I D U N G
der Technischen Beschwerdekammer 3.4.03
vom 21. Juni 2017

Beschwerdeführer: (Anmelder)
Giesecke & Devrient GmbH
Prinzregentenstrasse 159
81677 München (DE)

Vertreter:
Giesecke & Devrient GmbH
Patent- und Lizenzabteilung
Prinzregentenstrasse 159
81677 München (DE)

Angefochtene Entscheidung:
Entscheidung der Prüfungsabteilung des Europäischen Patentamts, die am 10. Mai 2012 zur Post gegeben wurde und mit der die europäische Patentanmeldung Nr. 99924992.3 aufgrund des Artikels 97 (2) EPÜ zurückgewiesen worden ist.

Zusammensetzung der Kammer:

Vorsitzender G. Eliasson
Mitglieder: M. Stenger
C. Schmidt

Sachverhalt und Anträge

I. Die Beschwerde betrifft die Zurückweisung der europäischen Patentanmeldung Nr. 99924992 durch die Prüfungsabteilung wegen mangelnder Einheitlichkeit nach Artikel 82 EPÜ.

II. Mit der Beschwerdebegründung reichte die Anmelderin einen neuen Hauptantrag und zwei Hilfsanträge ein.

III. In einer Mitteilung nach Regel 100(2) EPÜ vom 18.04.2017 teilte die Kammer der Anmelderin mit, dass der Einwand der mangelnden Einheitlichkeit in Anbetracht der geänderten Anträge nicht mehr zutreffe und dass auf Basis des Hauptantrags ein Patent erteilt werden könne, wenn einige andere Einwände hinsichtlich Gültigkeit der Priorität und Artikel 84 EPÜ ausgeräumt würden.

IV. Die Anmelderin änderte den Hauptantrag mit Schreiben vom 26. April 2017 und vom 16. Mai 2017 entsprechend. Sie beantragt die Erteilung eines Patents auf Basis folgender Unterlagen:

Beschreibung:
- Seiten 1 bis 12 und 15 bis 17 eingereicht mit Schreiben vom 26. April 2017
- Seiten 13 und 14 eingereicht mit Schreiben vom 16. Mai 2017

Ansprüche:
- 1 bis 5 und 6 (1. Teil) eingereicht mit Schreiben vom 26. April 2017
- 6 (2. Teil) und 7 bis 15 eingereicht mit Schreiben vom 16. Mai 2017

Zeichnungen:
- Blatt 1/4 bis 4/4 wie veröffentlicht

V. Es wird auf die folgenden Dokumente verwiesen:
D1: US 4 932 053 A
D2: XP002118740
D3: FR 2 745 924 A
D4: EP 0 908 810 A

VI. Die unabhängigen Ansprüche 1 und 9 lauten wie folgt:

1. Datenträger mit einem Halbleiterchip, der wenigstens einen Speicher aufweist, in dem ein Betriebsprogramm abgelegt ist, dadurch gekennzeichnet,
daß mit dem Betriebsprogramm eine Vielzahl von Operationen ausgeführt werden können,
wobei für wenigstens eine Untermenge dieser Operationen gilt, daß das bei Ausführung mehrerer Operationen der Untermenge erzielte Gesamtergebnis nicht von der Reihenfolge der Ausführung der Operationen abhängt,
und die Reihenfolge der Ausführung der genannten Untermenge von Operationen wenigstens dann variiert wird, wenn die Untermenge einen oder mehrere sicherheitsrelevante Operationen enthält.

9. Verfahren, in einem Datenträger mit einem Halbleiterchip, der wenigstens einen Speicher aufweist, in dem ein Betriebsprogramm abgelegt ist, zur Ausführung einer Vielzahl von Operationen innerhalb des Betriebsprogramms des Datenträgers,
wobei für wenigstens eine Untermenge dieser Operationen gilt, daß das bei Ausführung mehrerer Operationen der Untermenge erzielte Gesamtergebnis nicht von der Reihenfolge der Ausführung der Operationen abhängt,
und die Reihenfolge der Ausführung der genannten Untermenge von Operationen wenigstens dann variiert

wird, wenn die Untermenge einen oder mehrere sicherheitsrelevante Operationen enthält.

Entscheidungsgründe

1. Die Beschwerde ist zulässig.

2. Die vorliegende Anmeldung betrifft die Aufgabe, geheime Daten, die in einem Speicher eines Datenträgers (insbesondere einer Chipkarte) vorhanden sind, vor unberechtigtem Zugriff zu schützen.

Während der Ausführung eines Programms können unter Umständen von außerhalb Signalverläufe abgehört werden, die den vom Programm durchgeführten Operationen entsprechen. Diese Signalverläufe lassen nach einer Analyse gegebenenfalls einen Rückschluss auf die verwendeten geheimen Daten zu.
Die vorliegende Anmeldung verfolgt dabei nicht das Ziel, das Abhören der Signalverläufe an sich zu verhindern, sondern Rückschlüsse aus den Signalverläufen auf die geheimen Daten zu erschweren.

Die ursprüngliche Anmeldung verfolgte dazu drei verschiedene Ansätze.
In der aktuell vorliegenden Fassung ist die Anmeldung auf eine Variante beschränkt, in der die Reihenfolge der durchzuführenden Operationen unter bestimmten Umständen variiert wird. Dadurch wird das Programm nicht immer nach demselben Ablaufschema abgearbeitet. Aus diesem Grund hat ein möglicherweise die Signalverläufe abhörender Angreifer weniger Ansatzpunkte für eine Analyse der Signalverläufe, die Rückschlüsse auf die verwendeten Daten erlaubt.

3. Mangelnde Einheitlichkeit, Artikel 82 EPÜ 1973

Die Prüfungsabteilung hatte in der angefochtenen Entscheidung drei Gruppen von Erfindungen identifiziert.
Die Ansprüche des vorliegenden, geänderten Anspruchssatzes sind auf eine dieser Gruppen beschränkt. Diese Gruppe entspricht der in der ursprünglichen Anmeldung auf Seite 5, Zeile 20 bis Seite 6, Zeile 16 und Seite 15, Zeile 4 bis Seite 16, Zeile 22 in Verbindung mit Figur 5 beschriebenen Ausführungsform, nach der die Sicherheit eines Datenträgers erhöht wird, indem die Reihenfolge der Ausführung von Operationen variiert wird.

Der in der angefochtenen Entscheidung genannte Zurückweisungsgrund trifft daher nicht mehr zu.

4. Artikel 84 EPÜ 1973

Die Beschreibung wurde an die geänderten Ansprüche angepasst.

Die Kammer hat keine anderen Einwände in Bezug auf Artikel 84 EPÜ.

5. Artikel 123(2) EPÜ

Die unabhängigen Ansprüche 1 (Datenträger) und 9 (Verfahren) beruhen auf den ursprünglichen Ansprüchen 13 (Datenträger) und 34 (Verfahren).

Der ursprüngliche Anspruch 13 war dabei zwar als abhängiger Anspruch des unabhängigen Anspruchs 1 formuliert und enthielt daher Merkmale, die nicht im

vorliegenden Anspruch 1 enthalten sind. Der ursprüngliche Anspruch 34, der als unabhängiger Anspruch formuliert war, bietet jedoch eine Basis für die Streichung der Merkmale des ursprünglichen Anspruchs 1 im vorliegenden Anspruch 1.

Zusätzlich wurde in den vorliegenden Ansprüchen 1 und 9 ergänzt, dass es sich bei dem genannten Datenträger um einen Datenträger mit einem Halbleiterchip handelt, der wenigstens einen Speicher aufweist, in dem ein Betriebsprogramm abgelegt ist. Eine Grundlage hierfür findet sich zum Beispiel auf Seite 1, Zeilen 5 bis 6 und Seite 2, Zeilen 9 bis 10 der ursprünglichen Anmeldung (internationale A1-Veröffentlichung).

Die abhängigen Ansprüche 2 bis 8 sowie 10 bis 16 entsprechen den ursprünglichen Ansprüchen 14 bis 19 und 21 sowie 35 bis 40.

Die Erfordernisse des Artikels 123(2) sind daher erfüllt.

6. Priorität, Artikel 87 EPÜ 1973

In einem Bescheid vom 6. Dezember 2002 hatte die Prüfungsabteilung die Gültigkeit der beanspruchten Priorität in Frage gestellt. Diese Frage ist für die Bedeutung des Dokuments D4 im Verfahren wesentlich und wird daher hier behandelt.

Die vorliegende Anmeldung beansprucht die Priorität der deutschen Patentanmeldungen mit den Aktenzeichen 19822217.3, 19822220.3 und 19822218.1, die alle am 18. Mai 1998 eingereicht wurden.

Gegenstand der deutschen Anmeldung mit dem Aktenzeichen 19822218.1 ist ein Datenträger mit einem Halbleiterchip, der wenigstens einen Speicher aufweist, in dem ein Betriebsprogramm abgelegt ist, sowie ein entsprechendes Verfahren. Die Merkmale der vorliegenden Ansprüche werden in dieser Anmeldung offenbart (siehe Ansprüche 1 bis 8 der deutschen Anmeldung sowie Figur 3 und die dazugehörige Beschreibung).

Die Priorität der deutschen Anmeldung 19822218.1 vom 18. Mai 1998 wird daher gültig in Anspruch genommen.

7. Die Prüfungsabteilung hatte in einem Bescheid vom 6. Dezember 2002 bereits den Hinweis gegeben, dass eine Beschränkung der Anmeldung auf die Ausführungsform, in der die Reihenfolge von Operationen variiert wird, neu und erfinderisch sein könnte. Die Kammer schließt sich dieser Meinung aus den folgenden Gründen an.

8. Neuheit

8.1 D1 und D3

Die Dokumente D1 und D3 betreffen wie die vorliegende Anmeldung die Sicherheit von in elektronischen Speichern (Chipkarten) abgelegten vertraulichen Informationen.

Sowohl D1 als auch D3 zielen ebenso wie die vorliegende Anmeldung darauf ab, zu verhindern, dass aus während des Ablaufs eines Programms gegebenenfalls abgehörten Signalverläufen auf diese vertraulichen Informationen Rückschlüsse gezogen werden können (D1: siehe Zusammenfassung; D3: siehe Seite 2, Zeile 9 bis Seite 3, Zeile 5).

In den Worten der unabhängigen Ansprüche 1 und 9 offenbaren sowohl D1 als auch D3 zu diesem Zweck einen

Datenträger mit einem Halbleiterchip, der wenigstens einen Speicher aufweist, in dem ein Betriebsprogramm abgelegt ist, mit dem eine Vielzahl von Operationen ausgeführt werden kann, sowie ein entsprechendes Verfahren zur Ausführung der Operationen (D1: siehe Spalte 1, Zeile 10 bis 39 und Spalte 1, Zeile 66 bis Spalte 2, Zeile 3; D3: siehe Seite 1, Zeilen 10 bis 16).

Keines der Dokumente D1 und D3 offenbart jedoch ein Betriebsprogramm mit Operationen, deren Reihenfolge variiert werden kann.

Der Gegenstand der Ansprüche 1 und 9 der vorliegenden Anmeldung unterscheidet sich daher sowohl von D1 als auch von D3 dadurch, dass

a) für wenigstens eine Untermenge dieser Operationen gilt, dass das bei Ausführung mehrerer Operationen der Untermenge erzielte Gesamtergebnis nicht von der Reihenfolge der Ausführung der Operationen abhängt, und

b) die Reihenfolge der Ausführung der genannten Untermenge von Operationen wenigstens dann variiert wird, wenn die Untermenge einen oder mehrere sicherheitsrelevante Operationen enthält.

8.2 D2

Das Dokument D2 ist ein Auszug aus einem Standardlehrbuch über Kryptographie und beschäftigt sich allgemein mit der Verschlüsselung von Nachrichten mit Hilfe sogenannter *one-time pads*. Die oben genannten Merkmale a) und b) sind in D2 nicht offenbart.

8.3 D4

Das Dokument D4 betrifft, ähnlich wie die Dokumente D1 und D3, die Erhöhung der Sicherheit von in

elektronischen Speichern abgelegten vertraulichen Informationen (siehe [1] und [6]). Ein Schwerpunkt von D4 liegt auf der Sicherheit dieser Informationen während ihrer Übertragung (siehe [51]).
Zu diesem Zweck offenbart D4 einen Speicher (*storage device*), in dem ein Betriebsprogramm abgelegt ist (siehe zum Beispiel [9]). Dabei (siehe Figur 1 und [190-195]) wird die Reihenfolge von Operationen während ihrer Übertragung von einem externen Speicher (*external memory*) in einen Pufferspeicher (*block buffers* in einem *secure circuit*) variiert, nicht aber während der Ausführung durch die CPU (*lines of clear text* im *cache 140*).
Die oben genannten Merkmale a) und b) sind in D4 nicht offenbart.

8.4 Keines der Dokumente D1 bis D4 offenbart also die oben definierten Merkmale a) und b).

Der Gegenstand der unabhängigen Ansprüche der vorliegenden Anmeldung ist daher in Bezug auf den verfügbaren Stand der Technik neu nach Artikel 54 EPÜ.

9. Erfinderische Tätigkeit, Artikel 56 EPÜ 1973

9.1 D4

D4 beansprucht auf gültige Weise die Priorität der am 10. Oktober 1997 eingereichten amerikanischen Anmeldung US949111 (veröffentlicht als US6061449), wurde am 6. Oktober 1998 eingereicht und am 14. April 1999 veröffentlicht.
Da der 18. Mai 1998 gültig als Prioritätstag der vorliegenden Anmeldung beansprucht wird (siehe oben), stellt Dokument D4 Stand der Technik nach Artikel 54(3) EPÜ dar. D4 ist daher bei der Beurteilung der erfinderischen Tätigkeit nach Artikel 56 EPÜ nicht in Betracht zu ziehen.

9.2 D1, D2 und D3

Beide Dokumente D1 und D3 beschäftigen sich mit demselben Grundproblem wie die vorliegende Anmeldung (siehe Seite 2, Zeilen 17 bis 20), nämlich Daten auf einem Datenträger vor unberechtigtem Zugriff zu schützen. Die vorliegenden unabhängigen Ansprüche unterscheiden sich von jedem der beiden Dokumente durch dieselben Merkmale a) und b). Jedes der beiden Dokumente D1 und D3 eignet sich daher gleichermaßen als nächstliegender Stand der Technik für den Aufgabe-Lösungs-Ansatz.

Die Dokumente D1 und D3 enthalten Vorschläge zur Lösung des genannten Grundproblems, Daten auf einem Datenträger vor unberechtigtem Zugriff zu schützen.

D1 schlägt vor, dem durch die eigentlichen Operationen hervorgerufenen tatsächlichen Stromverbrauch einen pseudozufälligen Stromverbrauch zu überlagern (siehe Spalte 2, Zeilen 29 bis 45).
Dies hat den Nachteil, dass der Stromverbrauch insgesamt erhöht wird.

D3 (siehe Seite 8, Zeilen 2 bis 9, Seite 9, Zeilen 1 bis 21 sowie Seite 17, Zeile 32 bis Seite 18, Zeile 2) sieht vor, die Taktzeiten bei der Abarbeitung des Betriebsprogramms (*programme principal*) auf eine zufällige Weise variabel zu gestalten oder zusätzliche Operationen in zufälliger Weise durchzuführen (*programme secondaire).*
Dies hat den Nachteil, das die Ausführung des Betriebsprogramms (*programme principal*) insgesamt länger dauert (da minimale Taktzeiten berücksichtigt werden müssen, siehe Seite 8, Zeilen 2 bis 9 sowie Seite 18, Zeilen 2 bis 15).

Im Vergleich zu diesen Vorschlägen vermeidet die erfindungsgemäße Lösung des Grundproblems, Daten auf einem Datenträger vor unberechtigtem Zugriff zu schützen, mit den unterscheidenden Merkmalen a) und b) zusätzlich noch die Nachteile der in D1 und D3 vorgeschlagenen Lösungen.

Ausgehend von D1 oder D3 könnte die objektive technische Aufgabe so formuliert werden, dass eine alternative Lösung für das Grundproblem, Daten auf einem Datenträger vor unberechtigtem Zugriff zu schützen, gefunden werden soll, die mit weniger Nachteilen behaftet ist.
Anders formuliert sollen Rückschlüsse auf geheime Informationen aus beim Ablauf eines Betriebsprogramms gegebenenfalls abgehörten Signalverläufen auf eine andere Art als in D1 beziehungsweise D3 verhindert werden, die zudem weniger Nachteile aufweist.

Keinem der Dokumente D1 und D3 ist ein Hinweis zu entnehmen, dass die Reihenfolge von Operationen eines Betriebsprogramms bei der Ausführung variiert werden könnte.

D2 enthält ebenfalls keinen solchen Hinweis und betrifft darüber hinaus auch ein anderes Problem, so dass der Fachmann D2 nicht heranziehen würde, um ausgehend von D1 oder D3 die genannte objektive technische Aufgabe zu lösen.

Die Kammer ist auch nicht der Ansicht, dass die Variation der Reihenfolge von Operationen eines Betriebsprogramms zum Prioritätszeitpunkt der vorliegenden Anmeldung Bestandteil des allgemeinen Fachwissens war.

9.3 Aus diesen Gründen beruht der Gegenstand der unabhängigen Ansprüche 1 und 9 in Anbetracht des verfügbaren Standes der Technik auf einer erfinderischen Tätigkeit nach Artikel 56 EPÜ 1973.

Entscheidungsformel

Aus diesen Gründen wird entschieden:

1. Die angefochtene Entscheidung wird aufgehoben.

2. Die Angelegenheit wird an die erste Instanz mit der Anordnung zurückverwiesen, ein Patent mit folgender Fassung zu erteilen:

Beschreibung:
- Seiten 1 bis 12 und 15 bis 17 eingereicht mit Schreiben vom 26. April 2017
- Seiten 13 und 14 eingereicht mit Schreiben vom 16. Mai 2017

Ansprüche:
- 1 bis 5 und 6 (1. Teil) eingereicht mit Schreiben vom 26. April 2017
- 6 (2. Teil) und 7 bis 15 eingereicht mit Schreiben vom 16. Mai 2017

Zeichnungen:
- Blatt 1/4 bis 4/4 wie veröffentlicht

Die Geschäftsstellenbeamtin: Der Vorsitzende:

M. Schalow G. Eliasson

Entscheidung elektronisch als authentisch bestätigt