Interner Verteilerschlüssel:

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

Datenblatt zur Entscheidung vom 3. März 2016

Beschwerde-Aktenzeichen: T 2440/11 - 3.4.03

Anmeldenummer: 06753576.5

Veröffentlichungsnummer: 1883906

IPC: G07F7/10, H04L9/32

Verfahrenssprache: DE

Bezeichnung der Erfindung:
TRAGBARER DATENTRÄGER MIT SICHERER DATENVERARBEITUNG

Anmelder:
Giesecke & Devrient GmbH

Stichwort:

Relevante Rechtsnormen:
EPÜ 1973 Art. 56

Schlagwort:
Erfinderische Tätigkeit (ja) - Hauptantrag

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 2440/11 - 3.4.03

E N T S C H E I D U N G
der Technischen Beschwerdekammer 3.4.03
vom 3. März 2016

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

Angefochtene Entscheidung: **Entscheidung der Prüfungsabteilung des Europäischen Patentamts, die am 7. Juli 2011 zur Post gegeben wurde und mit der die europäische Patentanmeldung Nr. 06753576.5 aufgrund des Artikels 97 (2) EPÜ zurückgewiesen worden ist.**

Zusammensetzung der Kammer:

Vorsitzender G. Eliasson
Mitglieder: R. Bekkering
C. Schmidt

Sachverhalt und Anträge

I. Die Beschwerde richtet sich gegen die Entscheidung der Prüfungsabteilung, die Anmeldung Nr. 06 753 576 wegen fehlender erfinderischer Tätigkeit (Artikel 56 EPÜ) zurückzuweisen.

II. Die Anmelderin und Beschwerdeführerin hat in der mündlichen Verhandlung vor der Kammer beantragt, die angefochtene Entscheidung aufzuheben und ein Patent auf Grundlage der folgenden Dokumente zu erteilen:

Hauptantrag:

Ansprüche: 1 bis 36 gemäß Hauptantrag, eingereicht in der mündlichen Verhandlung vor der Kammer am 3. März 2016;

Beschreibung: Seiten 1 und 3 bis 19 in der veröffentlichten Fassung; Seiten 2 und 2a, eingereicht mit Schreiben vom 19. Januar 2016;

Zeichnungen: Figuren 1 bis 3 in der veröffentlichten Fassung.

oder hilfsweise auf Grundlage einer der Anträge 1 bis 4, eingereicht mit Schreiben vom 19. Januar 2016.

III. Anspruch 1 gemäß dem Hauptantrag lautet:

"*Verfahren zum sicheren Verarbeiten von Daten (22) in einem tragbaren Datenträger (1), wobei die folgenden Schritte in dem tragbaren Datenträger ausgeführt werden: a) Anfordern von zu verarbeitenden Daten (22);*

b) Verschlüsseln (S4) der zu verarbeitenden - von einem externen Gerät zur Verfügung gestellten - Daten (22);
c) Zwischenspeichern (S5) der verschlüsselten Daten (19) in einem nicht-flüchtigen Zwischenspeicherbereich (18) des Datenträgers (1);
d) Entschlüsseln (S6) der zwischengespeicherten, verschlüsselten Daten (19) mittels eines in dem Datenträger gespeicherten Entschlüsselungsschlüssels (17); und
e) Verarbeiten (S7) der entschlüsselten, zu verarbeitenden Daten (22),
wobei bei einer Unterbrechung (F1) während des Zwischenspeicherns nicht die bereits zwischengespeicherten Daten sondern der Entschlüsselungsschlüssel (17) gelöscht wird (F2)."

Anspruch 20 gemäß dem Hauptantrag lautet:

"*Tragbarer Datenträger (1), umfassend einen Prozessor (2), einen nichtflüchtigen Speicher (4) sowie eine Verarbeitungssteuerung (10) und eine Kryptographiefunktion (11), die beide von dem Prozessor (2) ausführbar sind, wobei*
- die Verarbeitungssteuerung (10) eingerichtet ist, zu verarbeitende Daten (22) anzufordern, ein Zwischenspeichern (S5) der zu verarbeitenden Daten (22) in einem Zwischenspeicherbereich (18) des Datenträgers (1) in verschlüsselter Form (19) zu bewirken und eine Verarbeitung der zwischengespeicherten, verschlüsselten Daten (19) als entschlüsselte Daten (15) zu bewirken, wobei die Verarbeitungssteuerung (10) so eingerichtet ist, dass bei einer Unterbrechung (F1) des Zwischenspeicherns nicht die bereits

zwischengespeicherten Daten sondern der Entschlüsselungsschlüssel (17) gelöscht wird (F2); und

- die Kryptographiefunktion (11) eingerichtet ist, die im Zwischenspeicherbereich (18) zwischenzuspeichernden, von einem externen Gerät zur Verfügung gestellten, Daten (22) zu verschlüsseln und die zu verarbeitenden, verschlüsselten Daten (19) mit einem in dem Datenträger gespeicherten Entschlüsselungsschlüssel (17) zu entschlüsseln."

IV. Es wird auf die folgenden Dokumente Bezug genommen:

D1: US2002/0114461 A

D2: US 6 715 078 B

D3: US2003/0056099 A

D4: EP 0 914 640 B.

V. Die Beschwerdeführerin machte im Wesentlichen Folgendes geltend:

Die zu verarbeitenden Daten des externen Gerätes werden erfindungsgemäß auf dem Datenträger verschlüsselt und in verschlüsselter Form zwischengespeichert. Somit bleiben die Daten auch unabhängig von ihrer Größe schnell löschbar durch Löschen des Entschlüsselungsschlüssels. Für die Verarbeitung der Daten werden die verschlüsselten Daten wieder entschlüsselt und bestimmungsgemäß verarbeitet (endgültig gespeichert). Die beanspruchte Lösung zeige also einen technischen Effekt in Form des schnellen Löschens für Daten, die in den nicht-flüchtigen Zwischenspeicherbereich gespeichert

werden.

Zudem, da weder Dokument D2 noch eines der weiteren Dokumente lehre, innerhalb der Karte Daten für die Ablage in einen Zwischenspeicherbereich zu verschlüsseln, um sie schneller löschen zu können, sei nicht erkennbar, wie oder erst recht warum der Fachmann in naheliegender Weise zu der vorgeschlagenen Lösung gelangen sollte.

Damit sei der Gegenstand der Ansprüche 1 und 20 gemäß dem Hauptantrag sowie den Hilfsanträgen nicht nur technisch sondern auch neu und beruhe auf einer erfinderischen Tätigkeit gegenüber dem zitierten Stand der Technik.

Entscheidungsgründe

1. Die Beschwerde ist zulässig.

2. Hauptantrag

2.1 Änderungen

Der Anspruch 1 basiert auf den ursprünglich eingereichten Ansprüchen 1 und 4, sowie auf der ursprünglich eingereichten Beschreibung (vgl. Seite 4, Zeilen 1 bis 4).

Der unabhängige Anspruch 20 basiert auf dem ursprünglich eingereichten Anspruch 20 und der ursprünglich

eingereichten Beschreibung (vgl. Seite 4, Zeilen 1 bis 4).

Der abhängige Anspruch 4 basiert auf der ursprünglich eingereichten Beschreibung (vgl. Seite 12, Zeilen 7 bis 8).

Die abhängigen Ansprüche 2, 3 und 5 bis 19 sowie 21 bis 36 entsprechen den jeweiligen ursprünglich eingereichten Ansprüchen.

Die Änderungen sind somit im Sinne von Artikel 123(2) EPÜ zulässig.

2.2 Neuheit

2.2.1 Dokument D4

Nach Auffassung der Kammer bildet das in der Anmeldung zitierte Dokument D4 den nächstliegenden Stand der Technik (vgl. Anmeldungsbeschreibung, Seite 2, Zeilen 10 bis 13).

Dokument D4 zeigt ein Verfahren zum Verarbeiten von Daten in einem tragbaren Datenträger (vgl. Absätze [0028] bis [0030]; Figuren 4 und 5).

Insbesondere zeigt D4 in der Terminologie des Anspruchs 1 ein Verfahren zum sicheren Verarbeiten von Daten (ISj) in einem tragbaren Datenträger (8), wobei die folgenden Schritte in dem tragbaren Datenträger ausgeführt werden:

a) Anfordern von zu verarbeitenden Daten (ISj)(vgl. Figur 4, Schritt 41);
b) Verschlüsseln der zu verarbeitenden - von einem externen Gerät zur Verfügung gestellten - Daten (vgl. Figur 4, Schritt 47);

c) Zwischenspeichern der verschlüsselten Daten (ISj) in einem nicht-flüchtigen Zwischenspeicherbereich des Datenträgers (8);
d) Entschlüsseln der zwischengespeicherten, verschlüsselten Daten (ISj) mittels eines in dem Datenträger gespeicherten Entschlüsselungsschlüssels (CPi) (vgl. Figur 5, Schritt 53); und
e) Verarbeiten der entschlüsselten, zu verarbeitenden Daten (ISj)(vgl. Figur 5, Schritt 54).

Weiter werden in D4 die entschlüsselten Daten gelöscht, indem die Versorgungsspannung für den flüchtigen Speicher am Ende der Kommunikation wegfällt (vgl. Absatz [0030]).

Zudem wird in D4 der Entschlüsselungsschlüssel gelöscht, wenn eine neuere Version vorhanden ist (vgl. Absatz [0033]).

Dokument D4 befasst sich jedoch weder mit einer möglichen Unterbrechung der Datenübertragung bzw. Zwischenspeicherung und eventuell dadurch entstehenden Dateninkonsistenzen noch mit der damit verbundenen Löschung der unvollständig übertragenen Daten aus dem Speicher des Datenträgers.

Nicht bekannt aus D4 ist somit, dass bei einer Unterbrechung während des Zwischenspeicherns nicht die bereits zwischengespeicherten Daten sondern der Entschlüsselungsschlüssel gelöscht wird.

Damit ist der Gegenstand des Anspruchs 1 gegenüber Dokument D4 neu (Artikel 54(1) EPÜ 1973).

2.2.2 Der Gegenstand des Anspruchs 1 ist im Übrigen auch gegenüber dem weiteren im Verfahren zitierten Stand der Technik, der weniger relevant ist, neu.

Dokument D1

Dokument D1 zeigt ein Verwaltungssystem für Computerprogrammkopien. Das System umfasst eine optische Platte mit dem Computerprogramm in verschlüsselter Form, eine Speicherkarte, ein Benutzergerät mit einem Festplattenlaufwerk, einem optischen Laufwerk und einem Speicherkarten-Lesegerät, sowie einen System-Server (vgl. Absätze [0032] bis [0079]; Figuren 1 bis 3). Auf der Speicherkarte werden Identifizierungsdaten und Verschlüsselungsschlüssel gespeichert und ggf. nach der Verwendung wieder gelöscht (vgl. Absätze [0112] bis [0174]).

Die Speicherkarte selbst ist nur als Speichermedium ausgelegt und hat keine Verschlüsselungs- oder Datenverarbeitungsfähigkeiten. Sie hat somit keine Relevanz für den Datenträger der vorliegenden Erfindung.

Dokument D2

Dokument D2 zeigt ein Verfahren zur sicheren Verschlüsslung einer PIN. Nach Eingabe der PIN an einem Kundentransaktionsterminal, wird diese an eine mit Verschlüsselungsmitteln ausgestatte Chipkarte übertragen, dort verschlüsselt und zurück an das Terminal gesendet. Die Chipkarte erzeugt einen Verschlüsselungsschlüssel (MSK) durch Verschlüsselung einer Kombination einer generierten Zufallszahl und der Seriennummern der Karte und des Geräts. Nach Speicherung des Verschlüsselungsschlüssels werden alle bei der Erzeugung des Verschlüsselungsschlüssels benutzten Daten

gelöscht (vgl. Spalte 5, Zeile 57 bis Spalte 7, Zeile 4; Figuren 3 und 4). Zudem werden, wenn ein unbefugter Eingriff detektiert wird, der Verschlüsselungsschlüssel und alle Daten gelöscht (vgl. Spalte 7, Zeile 5 bis Spalte 8, Zeile 28; Figur 5).

Es geht allerdings in D2 nicht darum, die empfangenen Daten (PIN) nach der Verschlüsselung zu entschlüsseln und zu verarbeiten. Zudem befasst D2 sich nicht mit dem Fall, dass bei dem Empfang der Daten eine Unterbrechung eintreten könnte und dadurch Daten nur unvollständig übertragen werden.

Dokument D2 ist somit ebenfalls nicht relevant für die vorliegende Erfindung.

Dokument D3

Dokument D3 zeigt ein Verfahren zur Verteilung von privaten und öffentlichen Verschlüsselungsschlüsseln für Chipkarten.

Das ausstellende System sendet einen verschlüsselten privaten Schlüssel und ein Zertifikat eines öffentlichen Schlüssels zu einem Benutzerterminal, das die Daten in die Chipkarte eingibt. Die Chipkarte speichert das Zertifikat des öffentlichen Schlüssels und entschlüsselt den verschlüsselten privaten Schlüssel durch eine auf einem symmetrischen Schlüssel basierende Verschlüsselung/Entschlüsselung und speichert den erhaltenen privaten Schlüssel (vgl. Absätze [0015] bis [0018]).

In Dokument D3 werden die empfangenen Daten nicht verschlüsselt, anschließend entschlüsselt und dann verarbeitet. Zudem befasst auch D3 sich nicht mit dem

Fall, dass bei dem Empfang der Daten eine Unterbrechung eintreten könnte und dadurch Daten nur unvollständig übertragen werden.

Somit ist auch Dokument D3 nicht relevant für die vorliegende Erfindung.

2.3 Erfinderische Tätigkeit

Die Prüfungsabteilung vertritt in der angefochtenen Entscheidung die Auffassung, dass die Ansprüche lediglich eine abstrakte Abfolge von Schritten beschreiben, welche an den Fachmann mit der Aufgabe herangetragen werden, diese zu implementieren. Hierbei werde ausdrücklich jedoch keine technische Aufgabe gelöst. Da somit weder ein technisches Problem noch eine technische Lösung herausgearbeitet werden können, sei der beanspruchte Gegenstand nicht erfinderisch.

Die Kammer teilt diese Auffassung der Vorinstanz nicht.

Die Anmeldungsbeschreibung führt Folgendes aus: "*Zum Verarbeiten von Daten von einem mit einem Prozessor ausgestatteten tragbaren Datenträger, die diesem von einer externen Einrichtung zur Verfügung gestellt werden, besitzt der Datenträger Schreibfunktionen, die die Daten in einen bestimmten Speicherbereich eines nichtflüchtigen Speichers des Datenträgers schreiben, beispielsweise in einen EEPROM-Speicher einer Chipkarte. Dies gilt zum beispielsweise* [sic] *für Chipkarten und SmartCards, die für Transaktionen an einem Terminal eines Point-of-Sale oder eines Kreditinstituts verwendet werden. Üblicherweise werden solche Daten anhand einer Speicheradresse bitweise in eine Zieldatei des Datenträgers geschrieben werden. Derartige nach ISO-IIC 7816-4 standardisierte Schreibkommandos für Chipkarten*

sind beispielsweise UPDATE-BINARY und WRITE-BINARY. Zumeist sind die dem Datenträger zur Verfügung gestellten Daten nicht mehr als 256 Byte lang. Falls der Vorgang des Übertragens der Daten auf den Datenträger unterbrochen wird, beispielsweise durch eine Unterbrechung der Stromversorgung, muss ein 256 Byte grosser Speicherbereich gelöscht werden, um Dateninkonsistenzen zu vermeiden und die Integrität des Datenträgers sicherzustellen. Dies gilt insbesondere bei Chipkarten deshalb, weil Daten durch Aufbringen von Ladungen auf Kondensatoren gespeichert werden und das Einschreiben von Datenbits in den EEPROM-Speicher bei bestimmten Schreibkommandos von den zu überschreibenden Bits bzw. den aktuellen Energieniveaus der Kondensatoren abhängig sein kann. Da die meisten nichtflüchtigen (EEPROM) Speicher in Seiten zu 64 Byte organisiert sind, ergibt sich für das Datenlöschen ein typischer Zeitbedarf von 3 ms x 256/64 = 12 ms. Dieser Zeitbedarf ist auch bei kontaktlos betriebenen Chip-Karten noch vertretbar. Beim Speichern von grösseren Datensätzen kann die Zeit für das Löschen des entsprechenden Speicherbereichs jedoch inakzeptabel lang werden. So wird bei einem Datensatz von 8 KByte bereits eine Löschzeit von 8192/64 x 3 ms = 384 ms benötigt"(vgl. Beschreibung, Seite 1, Zeile 6 bis Seite 2, Zeile 4).

Anspruch 1 definiert, dass die folgenden Schritte in dem tragbaren Datenträger ausgeführt werden:

a) Anfordern von zu verarbeitenden Daten (22);
b) Verschlüsseln (S4) der zu verarbeitenden - von einem externen Gerät zur Verfügung gestellten - Daten (22);
c) Zwischenspeichern (S5) der verschlüsselten Daten (19) in einem nicht-flüchtigen Zwischenspeicherbereich (18) des Datenträgers (1);

d) Entschlüsseln (S6) der zwischengespeicherten, verschlüsselten Daten (19) mittels eines in dem Datenträger gespeicherten Entschlüsselungsschlüssels (17); und
e) Verarbeiten (S7) der entschlüsselten, zu verarbeitenden Daten (22).

Nach Auffassung der Kammer sind all diese Schritte technisch, schon deswegen weil jeder Schritt den Einsatz entsprechender technischer Mittel wie Kryptographie- und Verarbeitungsmittel sowie Speicher auf dem Datenträger impliziert.

Zudem wird nach Auffassung der Kammer mit den beanspruchten Merkmalen und dabei insbesondere dem letzten Merkmal des Anspruchs 1 eine technische Aufgabe gelöst. Wie in dem vorstehenden Zitat aus der Beschreibung dargelegt, sind bei einer Unterbrechung der Datenübertragung zur Gewährleistung der Datenintegrität die bereits übertragenen, unvollständigen Daten aus dem Speicher des Datenträgers zu löschen. Die zu lösende Aufgabe ist dabei, die lange Speicherlöschzeiten, die sich ergeben, zu reduzieren. Dies stellt nach Auffassung der Kammer ein technisches Problem dar. Aber auch die beanspruchte Lösung, die daraus besteht, dass bei einer Unterbrechung während des Zwischenspeicherns nicht die bereits zwischengespeicherten Daten sondern der Entschlüsselungsschlüssel gelöscht wird, ist nach Auffassung der Kammer eine technische Lösung.

Im Übrigen sind auch gegenüber Dokument D4 als nächstliegendem Stand der Technik die zu lösende Aufgabe und deren Lösung technisch.

So besteht ausgehend von Dokument D4 die zu lösende Aufgabe darin, bei einer möglichen Unterbrechung der

Datenübertragung lange Speicherlöschzeiten zu vermeiden. Wie oben dargelegt handelt es sich nach Auffassung der Kammer hierbei um eine technische Aufgabe und ist auch die beanspruchte Lösung technisch.

Da keines der sich im Verfahren befindlichen Dokumente sich mit der vorstehenden Aufgabe befasst und sich kein Hinweis auf die beanspruchte Lösung finden lässt, ergibt sich das Verfahren gemäß Anspruch 1 für den Fachmann nicht in naheliegender Weise aus dem Stand der Technik.

Dasselbe gilt auch für den Gegenstand des unabhängigen Anspruchs 20, der auf einen entsprechenden tragbaren Datenträger gerichtet ist.

Damit beruht der jeweilige Gegenstand der Ansprüche 1 und 20 auf einer erfinderischen Tätigkeit im Sinne von Artikel 56 EPÜ 1973.

Die weiteren Ansprüche 2 bis 19 und 21 bis 36 sind abhängig von Anspruch 1 bzw. 20 und stellen besondere Weiterbildungen des Gegenstandes dieser Ansprüche dar. Die Gegenstände dieser Ansprüche beruhen somit ebenfalls auf einer erfinderischen Tätigkeit.

2.4 Die Beschreibung wurde an die gültigen Ansprüche angepasst und trägt dem vorliegenden Stand der Technik Rechnung, sodass auch in dieser Hinsicht die Erfordernisse des EPÜ erfüllt sind.

3. Bei dieser Sachlage erübrigt sich die Abhandlung der Hilfsanträge.

Entscheidungsformel

Aus diesen Gründen wird entschieden:

1. Die angefochtene Entscheidung wird aufgehoben.

2. Die Sache wird an die Prüfungsabteilung zurückverwiesen, mit der Anordnung ein Patent wie folgt zu erteilen:

   Ansprüche: 1 bis 36 gemäß Hauptantrag, eingereicht in der mündlichen Verhandlung vor der Kammer am 3. März 2016;

   Beschreibung: Seiten 1 und 3 bis 19 in der veröffentlichten Fassung; Seiten 2 und 2a, eingereicht mit Schreiben vom 19. Januar 2016;

   Zeichnungen: Figuren 1 bis 3 in der veröffentlichten Fassung.

Die Geschäftsstellenbeamtin: Der Vorsitzende:

S. Sánchez Chiquero G. Eliasson

Entscheidung elektronisch als authentisch bestätigt