BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS

BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE

CHAMBRES DE RECOURS DE L'OFFICE EUROPEEN DES BREVETS

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

E N T S C H E I D U N G
vom 2. August 2001

Beschwerde-Aktenzeichen: T 0928/96 - 3.4.1

Anmeldenummer: 93108119.4

Veröffentlichungsnummer: 0570924

IPC: G07F 7/10

Verfahrenssprache: DE

Bezeichnung der Erfindung:
Verfahren zur Authentifizierung eines Systemteiles durch einen anderen Systemteil in einem Informationsübertragungssystem bestehend aus einem Terminal und einer tragbaren Datenträgeranordnung

Anmelder:
Infineon Technologies AG

Einsprechender:
-

Stichwort:
Chipkarte/SIEMENS

Relevante Rechtsnormen:
EPÜ Art. 56, 123(2)

Schlagwort:
"Erfinderische Tätigkeit (nein)"

Zitierte Entscheidungen:
-

Orientierungssatz:

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Aktenzeichen: T 0928/96 - 3.4.1

E N T S C H E I D U N G
der Technischen Beschwerdekammer 3.4.1
vom 2. August 2001

Beschwerdeführer: Infineon Technologies AG
St.-Martin-Straße 53
D-81669 München (DE)

Vertreter: Epping Hermann & Fischer
Ridlerstraße 55
D-80339 München (DE)

Angefochtene Entscheidung: **Entscheidung der Prüfungsabteilung des Europäischen Patentamts, die am 20. Mai 1996 zur Post gegeben wurde und mit der die europäische Patentanmeldung Nr. 93 108 119.4 aufgrund des Artikels 97 (1) EPÜ zurückgewiesen worden ist.**

Zusammensetzung der Kammer:

Vorsitzender: U. G. O. Himmler
Mitglieder: H. K. Wolfrum
C. Rennie-Smith

Sachverhalt und Anträge

I. Die europäische Patentanmeldung Nr. 93 108 119.4 wurde durch die am 20. Mai 1996 zur Post gegebene Entscheidung der Prüfungsabteilung zurückgewiesen.

II. Die Zurückweisung wurde damit begründet, daß der Gegenstand des Anspruchs 1 insbesondere im Hinblick auf die folgenden Entgegenhaltungen nicht erfinderisch ist (Artikel 52 (1) und 56 EPÜ):

D1: EP-A-0 388 700

D2: IT Informationstechnik, Bd. 32, Nr. 1, Februar 1990, Seiten 64 bis 67; G. Kunde et al., "*Der neue Flughafen München - Sicherheit durch Chipkarten*"

D3: EP-A-0 203 542.

Darüber hinaus erwähnt die Entscheidung das in der Anmeldung zitierte Dokument:

D4: A. Beutelspacher et al., "*Chipkarten als Sicherheitswerkzeug*", Springer Verlag Berlin-Heidelberg-New York, 1991, Kapitel 4.1.2, Seiten 61 bis 65.

III. Der Beschwerdeführer hat gegen diese Entscheidung der Prüfungsabteilung mit Schreiben vom 30. Juli 1996, beim Europäischen Patentamt eingegangen am 30. Juli 1996, Beschwerde eingelegt und gleichzeitig die Beschwerdegebühr entrichtet. Mit einem am 30. September 1996 eingegangenen Schriftsatz wurde die Beschwerde

begründet. Gleichzeitig beantragte der Beschwerdeführer die Aufhebung des Zurückweisungsbeschlusses der Prüfungsabteilung und die Erteilung eines Patents mit geänderten Ansprüchen 1 - 9. Hilfsweise beantragte er, eine mündliche Verhandlung anzuberaumen.

IV. In einer Mitteilung der Kammer vom 31. Mai 2001 als Anlage zur Ladung für die mündliche Verhandlung äußerte die Kammer ihre vorläufige Meinung, daß der Gegenstand des Anspruchs 1 dem Erfordernis der Artikel 52 (1) und 56 EPÜ nicht genüge. In diesem Zusammenhang verwies die Kammer noch auf die im Recherchenbericht enthaltene Druckschrift:

D5: EP-A-0 252 849.

Darüber hinaus verwies die Kammer auf Offenbarungsmängel (Artikel 123 (2) EPÜ) und Klarheitsmängel (Artikel 84 EPÜ).

V. Am 2. August 2001 fand vor der Beschwerdekammer eine mündliche Verhandlung statt. Im Laufe der Verhandlung reichte der Beschwerdeführer einen neuen Anspruch 1 als Hauptantrag und einen weiteren Anspruch 1 als Hilfsantrag ein, die alle vorherigen Anträge ersetzten.

VI. Anspruch 1 des Hauptantrags hat folgenden Wortlaut:

"1. Verfahren zur Authentifizierung eines Systemteiles durch einen anderen Systemteil in einem Informationsübertragungssystem aus einem Terminal und einer tragbaren Datenträgeranordnung nach dem "Challenge-and-Response"-Prinzip, wobei ein Systemteil jeweils von Vorgang zu Vorgang verschiedene Fragedaten zum anderen Systemteil überträgt, diese Fragedaten im

anderen Systemteil mindestens abhängig von einem Algorithmus und einem geheimen Schlüssel zu Antwortdaten verändert werden, diese Antwortdaten dann zu dem die Fragedaten absendenden Systemteil zurückgesendet werden, die Fragedaten in dem diese bereitstellenden Systemteil ebenfalls mindestens abhängig von einem Algorithmus und einem Schlüssel zu Antwortdaten verändert werden und die beiden unterschiedlich erstellten Antwortdaten dann verglichen werden, wobei die Übereinstimmung der beiden Antwortdaten eine positive Authentifikation bedeuten,
dadurch gekennzeichnet,
daß vor Durchführung eines jeden Authentifikations-vorganges als eine elektronische Bedingung jeweils zusätzlich das Ändern des Zählerstandes eines nicht-flüchtigen Zählers mit begrenztem Zählumfang erfolgt sein muß, wobei die Häufigkeit, mit der diese Bedingung erfüllt wird, eingeschränkt ist."

Anspruch 1 des Hilfsantrags fügt am Ende des Anspruchs 1 gemäß Hauptantrag noch die Merkmale an,

"und daß die Fragedaten zusätzlich von einer bei jeder Authentifikationsprüfung sich ändernden Größe abhängen, wobei diese sich bei jeder Authentifikationsprüfung ändernde Größe der Zählerstand eines Zählers ist."

VI. Zur Stützung seines Hauptantrags hat der Beschwerde-führer im wesentlichen folgende Argumente geltend gemacht:

a) Die technische Aufgabe der vorliegenden Erfindung beziehe sich auf die Authentifizierung der **Chipkarte** als berechtigtes Systemteil eines Informations-übertragungssystems und nicht auf die Identifizierung eines **Benutzers**.

Aufgabe der Druckschrift D3 sei dagegen die Reduzierung des Datenflusses zwischen Endgerät und Zentralrechner, wobei nicht bei **jeder** Benutzung eine Datenübertragung zwischen Endgerät und Zentralrechner stattfindet. Ein wichtiger Unterschied gegenüber der vorliegenden Erfindung bestehe darin, daß zwischen Chipkarte und Endgerät **keine** Authentifizierung stattfindet, sondern nur eine Benutzeridentifizierung erfolgt. Das bedeute, daß, solange die Benutzeridentifizierung, die beispielsweise mittels einer PIN erfolgt, erfolgreich ist, eine gefälschte Chipkarte mit dem Endgerät Daten austauschen kann.

b) Der Unterschied zwischen dem erfindungsgemäßen Authentifizierungs-Verfahren und einer PIN-Überprüfung sei darin zu sehen, daß bei der PIN-Überprüfung **von außen** versuchsweise Daten eingegeben werden, wohingegen bei dem erfindungsgemäßen Authentifizierungs-Verfahren von Systemteilen **keine Eingaben von außen** erfolgen und daher auch keine Einflußnahme von außen möglich ist.

c) Keines der anderen Dokumente des nachgewiesenen Standes der Technik habe dem Fachmann die Lehre vermittelt, zusätzlich zur Verwendung eines geheimen Schlüssels und eines Algorithmuses das Verändern der Fragedaten in Antwortdaten von einer weiteren, durch das Ändern des Zählerstandes eines Zählers gegebenen Bedingung abhängig zu machen. Daher hätte der Fachmann allenfalls in Kenntnis der Erfindung bei einer rückschauenden Betrachtungsweise zum Gegenstand der Erfindung gelangen können.

Hinsichtlich der zusätzlichen Merkmale des Hilfsantrags machte der Anmelder geltend, daß gemäß der Druckschrift

D1 zur Generierung der Fragedaten nur die Zufallszahl variiert werde, wohingegen beim Anmeldungsgegenstand die Fragedaten von einer weiteren, variablen Größe abhingen.

Entscheidungsgründe

1. *Zulässigkeit der Beschwerde*

Die Beschwerde entspricht den Artikeln 106 bis 108 EPÜ sowie der Regel 64 EPÜ; sie ist daher zulässig.

2. *Änderungen* (Artikel 123 (2) EPÜ)

Die ursprüngliche Offenbarung der Merkmale im gültigen Anspruch 1 des Hauptantrages ergibt sich aufgrund der ursprünglichen Ansprüche 1, 2 und 6.

Die zusätzlichen Merkmale im Anspruch 1 des Hilfsantrages sind in den ursprünglichen Ansprüchen 10 und 11 offenbart.

Nach Auffassung der Kammer genügen somit die gültigen unabhängigen Ansprüche den Erfordernissen des Artikels 123 (2) EPÜ.

3. *Erfinderische Tätigkeit*

3.1 Die Neuheit des Anmeldungsgegenstandes gegenüber dem entgegengehaltenen Stand der Technik steht außer Zweifel. Es ist daher zu untersuchen, ob der Gegenstand des gültigen Anspruchs 1 gemäß Hauptantrag auf einer für die Erteilung eines Patents erforderlichen erfinderischen Tätigkeit beruht.

Ein nach einem "Challenge-and-Response"-Prinzip arbeitendes Verfahren mit den Merkmalen des Oberbegriffs des Anspruchs 1 ist aus jeder der Druckschriften D1 (vgl. den Anspruch 1 sowie die Figuren 1 und 2 mit zugehöriger Beschreibung) und D4 (vgl. insbesondere das Kapitel 4.1.2.1) bekannt. Somit ist zu untersuchen, ob es auf einer erfinderischen Tätigkeit beruht, das aus D1 bzw. D4 bekannte Verfahren durch folgende beiden Verfahrensmerkmale zu ergänzen:

- vor Durchführung eines jeden Authentifikations-vorganges muß als eine elektronische Bedingung jeweils zusätzlich das Ändern des Zählerstandes eines nicht-flüchtigen Zählers mit begrenztem Zählumfang erfolgt sein,

- wobei die Häufigkeit, mit der diese Bedingung erfüllt wird, eingeschränkt ist.

3.2 Gemäß dem aus D4 bekannten Verfahren erfolgt die Authentifizierung zweier Systemteile, d. h. Chipkarte und Rechner, nach dem "Challenge-and-Response"-Prinzip,

- indem ein Systemteil eine Zufallszahl (**RAND**), welche natürlicherweise von Vorgang zu Vorgang verschieden ist (siehe Seite 61, vorletzter Absatz, zweitletzter Satz), als Fragedaten zum anderen Systemteil überträgt,

- im anderen Systemteil diese Zufallszahl mittels eines geheimen Schlüssels $\mathbf{K_c}$ und eines Algorithmuses $\mathbf{f_{Kc}}$ zu Antwortdaten $\mathbf{AP_c}$ verändert und

- diese Antwortdaten $\mathbf{AP_c}$ zu dem die Fragedaten (**RAND**) absendenden Systemteil zurücksendet,

- wobei in dem die Fragedaten (**RAND**) bereitstellenden Systemteil ebenfalls in Abhängigkeit von einem Algorithmus $\mathbf{f_{KR}}$ und einem Schlüssel $\mathbf{K_R}$ die Fragedaten (**RAND**) zu Antwortdaten $\mathbf{AP_R}$ verändert werden und

- die beiden unterschiedlich erstellten Antwortdaten dann verglichen werden, wobei die Übereinstimmung der beiden Antwortdaten eine positive Authentifikation bedeutet.

Am Ende des Ablaufprotokolls zum Bild 4.2 auf Seite 62 enthält D4 die Aussage, daß die Kommunikation zwischen Rechner und Chipkarte abgebrochen wird, wenn die Authentifizierung nicht erfolgreich abläuft. Auf Seite 63, erster Satz, wird diese Aussage ergänzt durch den Hinweis, daß als Schutz gegen zufällige Fehler eine Wiederholung der Authentifizierung vorgesehen sein kann.

3.3 Diese Hinweise können für den fachkundigen Leser nur bedeuten, daß nach Übertragung der **CID** (**C**ard **I**dentification **D**ata) der Rechner zunächst feststellt, ob mit der verwendeten Karte bereits ein oder sogar ein zweiter, nicht-erfolgreicher Authentifizierungsvorgang stattgefunden hat, bevor er mit der Authentifizierungs-prozedur fortfährt, denn sonst könnte der Rechner die Wiederholungen der Authentifizierungsversuche nicht auf zwei Versuche beschränken.

Die dieser Maßnahme zugrundeliegende Problematik ist der Druckschrift D4 ebenfalls bereits ausdrücklich auf Seite 63, letzter Absatz, zu entnehmen, wo die Frage der kryptologischen Stärke eines solchen "Challenge-and-Response"-Systems diskutiert wird, nämlich wieviele Paare der zwischen den Systemen ausgetauschten Daten

- Zufallszahl **RAND** und Antwort $\mathbf{AP_c}$ - man braucht, um für eine beliebige Zufallszahl **RAND** die Antwort $\mathbf{AP_c}$ vorhersagen zu können. Aus diesen Überlegungen zur Systemsicherheit ergibt sich zwangsläufig die Forderung nach einer Begrenzung der Zahl der Authentifizierungsversuche, welche in D4 ja auch schon konkret angesprochen ist. Um jedoch, wie vorgeschlagen, die Zahl der Authentifizierungsversuche auf **eine** Wiederholung begrenzen zu können, muß zwingend eine Vorrichtung oder Maßnahme vorgesehen sein, durch welche die zu einer bestimmten **CID** gehörigen, nicht-erfolgreichen Authentifizierungsversuche gezählt werden. Damit liegt es aber auf der Hand, daß nur durch die Änderung des Zählerstandes eines notwendigerweise nicht-flüchtigen Zählers während der Durchführung eines Authentifizierungsversuches das System erkennen kann, ob mit der verwendeten Chipkarte (**CID**) bereits ein oder zwei nicht-erfolgreiche Authentifizierungsversuche durchgeführt wurden. Ebenso ist es unmittelbar einsichtig, daß auch der Zählumfang des Zählers auf "***X + zwei***" ab einem Startwert "***X***" begrenzt sein muß und nach jedem erfolgreichen Authentifizierungsversuch der Zähler auf den Startwert "***X***" zurückzustellen ist. Somit ist die Häufigkeit, mit der die elektronische Bedingung "***X***" erfüllt wird, eingeschränkt.

3.4 Aus den genannten Gründen ist die Kammer davon überzeugt, daß sich die Merkmale des kennzeichnenden Teiles des Anspruchs 1 des vorliegenden Hauptantrages für den Fachmann aufgrund einfacher Schlußfolgerungen aus den Hinweisen in D4 ergeben, wonach bei einem nicht-erfolgreichen Authentifizierungsversuch der Rechner die Kommunikation abbricht, jedoch zum Schutz gegen zufällige Fehler eine Wiederholung der Authentifi-

zierungsprozedur vorgesehen werden kann.

Die Kammer wird in dieser Überzeugung noch dadurch bestärkt, daß es sich bei der Druckschrift D4 um ein Lehrbuch handelt, welches in dem zitierten Kapitel Grundprinzipien der Sicherheit von Chipkartensystemen behandelt, deren konkrete bauliche Verwirklichung dem Basiswissen des fachkundigen Lesers überlassen bleibt. Aus diesem Grunde ist die Kammer auch der Überzeugung, daß die unter Punkt 3.3 dargelegten Überlegungen keine rückschauende Betrachtung in Kenntnis der Erfindung darstellen.

3.5 Aufgrund der unter den Punkten 3.2 bis 3.4 dargelegten Ausführungen beruht der Gegenstand des Anspruchs 1 gemäß Hauptantrag nicht auf einer erfinderischen Tätigkeit gegenüber dem Stand der Technik gemäß der Druckschrift D4.

3.6 Aber auch der Gegenstand des Hilfsantrags, der sich durch die zusätzlichen Merkmale

"und daß die Fragedaten zusätzlich von einer bei jeder Authentifikationsprüfung sich ändernden Größe abhängen, wobei diese sich bei jeder Authentifikationsprüfung ändernde Größe der Zählerstand eines Zählers ist"

vom Gegenstand gemäß Anspruch 1 des Hauptantrags unterscheidet, beruht nicht auf einer erfinderischen Tätigkeit, wie im folgenden dargelegt wird:

3.7 Aus der Druckschrift D1 (vgl. Spalte 2, Zeilen 9 bis 15 und Spalte 2, Zeile 46 bis Spalte 3, Zeile 9) ist nämlich bekannt, daß für die Generierung eines variablen Startwertes s_i für eine neue Zufallszahl $v2_i$ der vom

Teilnehmer "A" - aus der vom Teilnehmer "B" übertragenen Zufallszahl $v1_{(i-1)}$, dem Schlüssel K und dem Chiffrier-Algorithmus f - generierte Autorisierungsparameter $AP1_{(i-1)}$ mit der vom Teilnehmer "A" beim Authentifikationsvorgang (i-1) zwischengespeicherten Zufallszahl $v2_{(i-1)}$ zur Bildung des neuen Startwertes s_i verknüpft wird und dieser modifizierte Startwert s_i zur Bildung der neuen Zufallszahl $v2_i$ benutzt wird. Diese Zufallszahl $v2_i$ wird ihrerseits wieder zwischengespeichert und an den Teilnehmer "B" übertragen.

Dieser aus der Druckschrift D1 bekannte Vorgang entspricht aber dem zusätzlichen Merkmal des Hilfsantrags, wonach die neuen Fragedaten ($v2_i$) zusätzlich von einer bei jeder Authentifikationsprüfung (i-1) sich - mit dem Autorisierungsparameter $AP1_{(i-1)}$ - ändernden Größe s_i abhängen. Das weitere Erfordernis, für diese Größe den Zählerstand eines Zählers zu verwenden, stellt eine konkretisierte Ausführungsform des aus D1 bekannten allgemeinen Prinzips dar, die Fragedaten in Abhängigkeit von einem gespeicherten variablen Startwert zu ermitteln.

Nachdem die Druckschriften D1 und D4 sich beide auf ein gattungsgemäßes Authentifizierungsverfahren beziehen und mit der Verbesserung der kryptologischen Sicherheit beschäftigen, hat es sich unmittelbar angeboten, das aus der Druckschrift D4 ableitbare Verfahren zum Zwecke der weiteren Erhöhung der kryptologischen Stärke gemäß dem Vorschlag aus der Druckschrift D1 weiterzubilden, zumal in der Druckschrift D4 die Problematik der begrenzten kryptologischen Stärke von "Challenge-and-Response"-Verfahren ausdrücklich angesprochen wird, und mit der Verwirklichung der zusätzlichen Maßnahme keine synergistische Wechselwirkung mit den übrigen Maßnahmen

zur Erhöhung der Systemsicherheit verbunden ist. Dabei hat nach Auffassung der Kammer die Verwendung des Zählerstandes eines Zählers als weitere Größe als einfachste technische Realisierung der der Druckschrift D1 entnehmbaren Lehre, die Generierung der Zufallszahl von einem zwischengespeicherten variablen Startwert abhängig zu machen, nahegelegen.

3.8 Somit beruht auch der Gegenstand des Anspruch 1 gemäß Hilfsantrag nicht auf einer erfinderischen Tätigkeit gegenüber dem Stand der Technik gemäß den Druckschriften D1 und D4.

4. Die abhängigen Ansprüche teilen das Schicksal der nicht erfinderischen unabhängigen Ansprüche 1 gemäß Haupt- und Hilfsantrag, auf die sie rückbezogen sind.

5. Damit erfüllen weder der Hauptantrag noch der Hilfsantrag die Erfordernisse der Artikel 52 (1) und 56 EPÜ und sind somit nicht gewährbar.

Entscheidungsformel

Aus diesen Gründen wird entschieden:

Die Beschwerde wird zurückgewiesen.

Der Geschäftsstellenbeamte: Der Vorsitzende:

R. Schumacher U. Himmler