Interner Verteilerschlüssel:

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

Datenblatt zur Entscheidung vom 7. November 2019

Beschwerde-Aktenzeichen: T 1960/13 - 3.5.01

Anmeldenummer: 09015883.3

Veröffentlichungsnummer: 2209084

IPC: G06Q20/00, G06F21/00

Verfahrenssprache: DE

Bezeichnung der Erfindung:
Manipulationssicherheit eines Endgeräts

Anmelder:
Giesecke+Devrient Mobile Security GmbH

Stichwort:
Manipulationssicherheit eines Endgerätes / GIESECKE+DEVRIENT MOBILE SECURITY GMBH

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

Schlagwort:
Erfinderische Tätigkeit - Hauptantrag - portabler Datenträger (nein - allgemein bekannt)
Änderungen - Hilfsantrag - unzulässige Erweiterung (ja)

Zitierte Entscheidungen:

Orientierungssatz:

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern

Boards of Appeal

Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Beschwerde-Aktenzeichen: T 1960/13 - 3.5.01

E N T S C H E I D U N G
der Technischen Beschwerdekammer 3.5.01
vom 7. November 2019

Beschwerdeführerin: (Anmelderin)	Giesecke+Devrient Mobile Security GmbH Prinzregentenstraße 159 81677 München (DE)
Vertreter:	Giesecke+Devrient Mobile Security GmbH Patente und Lizenzen Prinzregentenstraße 159 81677 München (DE)
Angefochtene Entscheidung:	**Entscheidung der Prüfungsabteilung des Europäischen Patentamts, die am 26. April 2013 zur Post gegeben wurde und mit der die europäische Patentanmeldung Nr. 09015883.3 aufgrund des Artikels 97 (2) EPÜ zurückgewiesen worden ist.**

Zusammensetzung der Kammer:

Vorsitzender	M. Höhn
Mitglieder:	N. Glaser
	P. Schmitz

Sachverhalt und Anträge

I. Die Beschwerde richtet sich gegen die Entscheidung der Prüfungsabteilung, mit der die europäische Patentanmeldung Nr. 09015883.3 aufgrund des Artikels 97(2) EPÜ mangels erfinderischer Tätigkeit (Artikel 56 EPÜ) zurückgewiesen wurde.

II. Die Prüfungsabteilung war insbesondere der Auffassung, dass Anspruch 1 des Hauptantrages nicht erfinderisch sei gegenüber der EP1168138 (D1) in Verbindung mit allgemeinem Fachwissen, wie z.B. aus Walter Hinz, Network Connectivity mit der Internet Smart Card, 7 Februar 2007 (D2) bekannt. Anspruch 1 des ersten bis dritten Hilfsantrages wurde ebenfalls als nicht erfinderisch erachtet.

III. In ihrer Beschwerdebegründung vom 20. August 2013 beantragte die Beschwerdeführerin die angefochtene Entscheidung aufzuheben und ein Patent zu erteilen auf der Grundlage des Hauptantrages oder des ersten oder zweiten Hilfsantrages, die hiermit eingereicht wurden. Hilfsweise wurde mündliche Verhandlung beantragt.

IV. In der Ladung zur mündlichen Verhandlung legte die Kammer ihre vorläufige Meinung dar, wonach sie mit den von der Prüfungsabteilung in der Zurückweisung dargelegten Gründen im Wesentlichen übereinstimmte und die Zurückweisung als gerechtfertig ansah. Des weiteren war die Kammer der vorläufigen Meinung, dass Anspruch 1 des Hauptantrages, wie auch aller Hilfsanträge, nicht den Erfordernissen des Artikels 123(2) EPÜ genügte.

V. Mit Schreiben vom 4. September 2019 legte die Beschwerdeführerin einen neuen Hauptantrag b, sowie neue Hilfsanträge 1b bis 3b vor.

VI. Am 7. November 2019 fand die mündliche Verhandlung statt, in deren Verlauf ein neuer Hauptantrag und ein neuer erster Hilfsantrag eingereicht wurden. Alle anderen Anträge wurden zurückgenommen. Am Ende der mündlichen Verhandlung verkündete der Vorsitzende die Entscheidung.

VII. Anspruch 1 des Hauptsantrages lautet wie folgt (Merkmalsgliederung (i), (ii), (iii-1) bis (iii-4) durch die Kammer):

"1. Verfahren auf einem Datenträger (20) zum Prüfen einer Manipulationssicherheit eines Endgeräts (10), mit dem der Datenträger (20) als eine Transaktionseinheit (23) verbunden ist, wobei
der Datenträger (20) als Transaktionseinheit reale Transaktionsdaten (R2) von dem Endgerät (10) entgegennimmt,
wobei die realen Transaktionsdaten (R2) als Realtransaktionsdaten (R3) von dem Datenträger (20) an einen Transaktionsserver (17) weitergeleitet werden;
dadurch gekennzeichnet, dass

(i) der Datenträger ein portabler Datenträger ist;

(ii) die realen Transaktionsdaten eine von einem Benutzer des Endgeräts beabsichtigte und veranlasste reale Transaktion definieren;

(iii) die Manipulationssicherheit des Endgeräts (10) für die reale Transaktion mittels zumindest einer zusätzlichen Pseudotransaktion geprüft wird, indem:

(iii-1) - der Datenträger (20) mit dem Endgerät (10) zusätzlich als Benutzer-Eingabeeinheit (22), verbunden ist, wobei sich der Datenträger (20) mittels der

Benutzer-Eingabeeinheit (22) gegenüber dem Endgerät (10) als Tastatur, Maus oder dergleichen anmelden kann,

(iii-2) - der Datenträger (20) als Benutzer-Eingabe-einheit (22) Pseudotransaktionsdaten (P1) an das Endgerät (10) übergibt, die reale Transaktionsdaten nachbilden oder simulieren und vom Endgerät (10) als Pseudotransaktionsdaten (P2) an den Datenträger (20) weitergeleitet werden, wobei die an das Endgerät (10) übergebenen Pseudotransaktionsdaten (P1) aber nur zum Prüfen der Manipulationssicherheit des Endgeräts (10) vorgesehen sind,

(iii-3) - der Datenträger (20) vom Endgerät (10) entgegengenommenen Pseudotransaktionsdaten (P2) nicht an den Transaktionsserver (17) weiterleitet und

(iii-4) - der Datenträger (20) prüft, ob als Transaktionseinheit (23) von dem Endgerät (10) entgegengenommene Pseudotransaktionsdaten (P2) im Vergleich zu den dem Endgerät (10) zuvor als Benutzer-Eingabeeinheit übergebenen Pseudotransaktionsdaten (P1) unmanipuliert sind."

Anspruch 1 des ersten Hilfsantrages basiert auf dem Anspruch 1 des Hauptantrages mit dem zusätzlichen Merkmal des ursprünglichen Hilfsantrags 3b, wie folgt:

"wobei der Datenträger (20) die Manipulationssicherheit des Endgeräts (10) feststellt, falls die übergebenen und die entgegengenommenen Pseudotransaktionsdaten (P1, P2) übereinstimmen."

Entscheidungsgründe

1. Anmerkungen zur Erfindung

1.1 Die Erfindung betrifft ein Verfahren zum Prüfen der Manipulationssicherheit eines Endgeräts mittels eines portablen Datenträgers ("Internet Smart Card"). Der portable Datenträger wird über eine USB-Schnittstelle an das Endgerät angeschlossen und erfüllt zwei Funktionen: zum einen dient er als "Eingabeeinheit" und zum anderen als "Transaktionseinheit". Der portable Datenträger enthält weiterhin einen Speicher und vorzugsweise einen eigenen Webserver.

1.2 In seiner Funktion als "Transaktionseinheit (23)" dient der portable Datenträger der Transaktionssicherheit bei vom Benutzer ausgeführten Transaktionen mit einem Bankserver. Es werden auf dem Endgerät sogenannte *"Realtransaktionsdaten"* oder *"reale Transaktionsdaten"* (R1), z.B. vom Benutzer mittels einer an das Endgerät (10) angeschlossenen Tastatur eingegeben, siehe Seite 16, Zeilen 26ff. Die Daten (R1) werden von einer auf dem Endgerät laufenden Anwendung entgegengenommen, Daten (R2). Sie definieren eine vom Bankserver ausführbare Transaktion. Im Falle einer Online-Überweisung sind die *"realen Transaktionsdaten"* die Authentisierungsdaten des Benutzers, oder die Überweisungsdaten, wie der Überweisungsbetrag oder eine Transaktionsnummer. Die erfassten Daten (R2) können zwischengespeichert werden und werden dann als Daten (R3) über eine gesicherte Leitung an einen Bank-Server übermittelt.

1.3 In seiner Funktion als "Benutzer-Eingabeeinheit (22)" stellt der portable Datenträger über eine Steuerapplikation sogenannte *"Pseudotransaktionsdaten"* zur Ver-

fügung, die an das Endgerät übermittelt (P1) und anschließend wieder empfangen werden (P2). Durch einen Vergleich (CMP) dieser beiden Datensätze (P1, P2) miteinander kann bei Abweichung festgestellt werden, ob Schadsoftware auf dem Endgerät Daten manipuliert hat. Die "*Pseudotransaktionsdaten*" (P1, P2) dienen also dazu, die Manipulationssicherheit des Endgeräts 10 festzustellen, indem Veränderungen der Eingabedaten durch Schadsoftware erkannt werden.

1.4 Die Anmeldung lässt offen, worin sich die Daten R1, R2 und R3 unterscheiden bzw. was nach der Eingabe mit den Daten auf dem Endgerät passiert. Nach der Eingabe der Daten durch den Benutzer könnte z.B. ein Zeitstempel zu den Daten hinzugefügt werden. Die Beschwerdeführerin führte aus, dass der Unterschied zwischen den Daten R1 und R2 grundsätzlich der gleiche sei, wie zwischen den Daten P1 und P2, denn letztere würden sich, wenn keine Manipulation vorliegt, ebenfalls nicht signifikant voneinander unterscheiden, siehe 20, zweiter Absatz, der Anmeldung.

2. Hauptantrag - Artikel 56 EPÜ

2.1 Anspruch 1 des Hauptantrages vom 30. Juli 2012 wurde mangels erfinderischer Tätigkeit gegenüber der D1 und allgemeinem Fachwissen zurückgewiesen. Der Unterschied von Anspruch 1 zu D1 wurde in der Ausgestaltung des Tokens der D1 als "portabler Datenträger" (Merkmal (i)) gesehen. Eine derartige Ausgestaltung wurde von der Prüfungsabteilung als allgemein bekannt, z.B. als "Internet Smartcard" der D2, angesehen.

2.2 Nach Meinung der Beschwerdeführerin unterscheidet sich Anspruch 1 des Hauptantrages von D1 zusätzlich durch die Merkmale (ii), (iii), (iii-1) bis (iii-4).

3. Die Kammer schließt sich der Meinung der Prüfungsabteilung an und befindet, dass sich Anspruch 1 von der D1 allein durch Merkmal (i) unterscheidet. Die Merkmale (ii), (iii), (iii-1) bis (iii-4) können aus nachfolgenden Gründen keinen Unterschied zur D1 begründen.

3.1 D1 offenbart ein Verfahren, wobei mittels eines Datenträgers, eines sogenannten Sicherheits-Token 102, die Manipulationssicherheit eines Endgerätes 101 überprüft wird. Es geht darum, sogenannte "Man-in-the-Middle" Attacken, siehe Absatz [0004], zu erkennen, wo ein Trojaner Daten im Datenaustausch verändert.

3.2 Das Merkmal (ii) ist aus der D1 bekannt. Das Endgerät 101 führt eine Anwendung 201 aus, die ein "Clearing" von Finanztransaktionen durchführt, die den beanspruchten *"realen Transaktionsdaten"* entsprechen, denn auf der Datenebene ist es nicht mehr erkennbar, ob und wo ein Benutzer diese Daten eingegeben hat. Das "Endgerät" nach Anspruch 1 empfängt, verarbeitet und sendet Daten, und derartige Funktionen führt auch das Endgerät 101 der D1 aus.

3.3 Das Merkmal (iii-1) ist in der beanspruchten Breite ebenfalls aus der D1 bekannt. Der Token der D1 verhält sich gegenüber dem Endgerät 101 wie eine "Benutzer-Eingabeeinheit", die Daten an das Endgerät 101 liefert. Er erhält Daten von einer auf dem Endgerät 101 laufenden Anwendung 201, verschlüsselt diese Daten mit einem auf dem Token gespeicherten Schlüssel und sendet die verschlüsselten Daten zurück an die Anwendung. Der Token ist zwar keine Tastatur oder Maus, er verhält sich aber als "*dergleichen*" gegenüber dem Endgerät, indem er Daten für das Endgerät bereitstellt.

3.4 Die Merkmale (iii), (iii-2) und (iii-3) sind auch aus der D1 bekannt.

Die Manipulationssicherheit des Endgeräts für eine reale Transaktion wird sichergestellt, indem der Token, wie in Abbildung 7c der D1 dargestellt, auf der Basis der vom Endgerät 101 an ihn übermittelten Transaktionsdaten eine "challenge" generiert und diese an einen Wächtercomputer ("guard") zur Analyse sendet, siehe Absatz [0008] bis [0011], [0025] und [0026]. Der Wächtercomputer generiert nun für unproblematische Transaktionen eine "reply" oder "challenge response", siehe Absatz [0024] und [0025], und sendet diese an den Token zur Überprüfung zurück, siehe Absatz [0022], [0023] und [0025]. Bei erfolgreicher Überprüfung autorisiert der Token die Transaktion.

Die "challenge" wird auf der Basis der realen Daten generiert, sie enthält die realen Transaktionsdaten und dient alleine dem Prüfen der Manipulationssicherheit des Endgeräts. Absatz [0011] und [0022] führen aus, dass die "challenge", u.a., einen monetären Betrag, einen Zeitstempel und den Auftraggeber enthält. Dies entspricht der Vorgehensweise der vorliegenden Erfindung: nach Abbildung 1 und Seite 22, letzter Absatz, der Anmeldung werden die *"Pseudotransaktionsdaten"* (P1) automatisch vorbereitet (GEN).

Die "challenge response" ist wiederum eine Funktion der "challenge", siehe Absatz [0024] von D1. Sie ist indikativ für die Transaktionsdaten und bestimmt die Autorisierung oder Nicht-Autorisierung der Transaktion für die die "challenge" generiert wurde, s. Absatz [0011]. Damit entspricht die "challenge" den Pseudotransaktionsdaten (P1) und die "challenge response" den Pseudotransaktionsdaten (P2).

Nach der Anmeldung, Seite 23, zweiter und dritter Absatz, umfasst die Erfindung ebenfalls eine Verschränkung von Pseudotransaktionsdaten und Realtransaktionsdaten, da beide gleichzeitig erfasst werden. Die von der Beschwerdeführerin angeführte klare Trennung zwischen diesen Daten ist damit nicht gegeben.

3.5 Das Merkmal (iii-4) ist so allgemein gefasst, dass es auf die D1 gelesen werden kann. Das Merkmal besagt nur, dass der Datenträger eine Manipulationsprüfung durchführt, was der Token in der D1 ebenfalls tut. Entgegen dem Argument der Beschwerdeführerin schließt es aber - der Gegenstand des Anspruches 1 ist ein Verfahren - den Einsatz von Wächtercomputern als eine gesonderte dritte Instanz nicht aus. Diese Instanz führt eine Plausibilitätsprüfung der in der übermittelten "challenge" referenzierten Transaktion durch, siehe Absatz [0025] und [0026], generiert eine "challenge response" und übermittelt diese zurück an den Token, der eine abschließende Prüfung durchführt.

3.6 Der Unterschied zwischen Anspruch 1 und D1 beschränkt sich somit auf die Ausgestaltung des Tokens als portablen Datenträger (Merkmal (i)). Eine derartige Ausgestaltung ist aber für ein derartiges Token aus dem allgemeinen Fachwissen nahegelegt, wie z.B. aus der D2 bekannt, das eine Internet-Smartcard offenbart.

3.7 Der Gegenstand des Anspruchs 1 beruht somit nicht auf einer erfinderischer Tätigkeit (Artikel 56 EPÜ) gegenüber der D1 und allgemeinem Fachwissen.

4. Hilfsantrag - Artikel 123(2) EPÜ

4.1 Der Hilfsantrag genügt nicht den Erfordernissen des Artikels 123(2) EPÜ, da das Merkmal "*wobei der*

Datenträger (20) die Manipulationssicherheit des Endgeräts (10) feststellt, falls die übergebenen und die entgegengenommenen Pseudotransaktionsdaten (P1, P2) übereinstimmen" über den Offenbarungsgehalt der ursprünglichen Anmeldung hinausgeht.

4.2 Die Beschwerdeführerin verwies auf den ursprünglichen Anspruch 3 und auf die Beschreibung, Seite 20, Zeilen 21 bis 23.

4.3 Im genannten Merkmal wurde der Begriff "im wesentlichen" gestrichen, woraus sich ein neuer technischer Zusammenhang ergibt, nämlich, dass auf Identität der Daten P1 und P2 geprüft wird. Allerdings wird in der Anmeldung, u.a. in der genannten Passage, bei der Überprüfung auf Datenmanipulation nur überprüft, ob die Daten P1 und P2 signifikant von einander abweichen. Auf Übereinstimmung der Daten P1 und P2 wird nicht geprüft.

4.4 Damit stellt dies eine unzulässige Änderung im Sinne des Artikels 123(2) EPÜ dar.

5. Im Ergebnis erfüllt keiner der beiden Anträge die Erfordernisse des EPÜ.

Entscheidungsformel

Aus diesen Gründen wird entschieden:

Die Beschwerde wird zurückgewiesen.

Der Geschäftsstellenbeamte: Der Vorsitzende:

T. Buschek M. Höhn

Entscheidung elektronisch als authentisch bestätigt