Interner Verteilerschlüssel:

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

Datenblatt zur Entscheidung vom 19. Dezember 2016

Beschwerde-Aktenzeichen: T 1304/12 - 3.5.03

Anmeldenummer: 06020952.5

Veröffentlichungsnummer: 1777911

IPC: H04L29/06

Verfahrenssprache: DE

Bezeichnung der Erfindung:
System und Speichermedium zur Bereitstellung einer sicheren Kommunikation von einem in einem gesicherten Netzwerk nicht eingebundenen Client-Computer

Anmelder:
Saynet Solutions GmbH

Stichwort:
Speichermedium zum Bereitstellen einer sicheren Kommunikation/ SAYNET

Relevante Rechtsnormen:
EPÜ Art. 56

Schlagwort:
Erfinderische Tätigkeit - (nein)

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 1304/12 - 3.5.03

E N T S C H E I D U N G
der Technischen Beschwerdekammer 3.5.03
vom 19. Dezember 2016

Beschwerdeführer: (Anmelder)	Saynet Solutions GmbH Josef-Scheidl-Strasse 12 85221 Dachau (DE)
Vertreter:	Grünecker Patent- und Rechtsanwälte PartG mbB Leopoldstraße 4 80802 München (DE)
Angefochtene Entscheidung:	**Entscheidung der Prüfungsabteilung des Europäischen Patentamts, die am 5. Januar 2012 zur Post gegeben wurde und mit der die europäische Patentanmeldung Nr. 06020952.5 aufgrund des Artikels 97 (2) EPÜ zurückgewiesen worden ist.**

Zusammensetzung der Kammer:

Vorsitzender	F. van der Voort
Mitglieder:	K. Schenkel
	O. Loizou

Sachverhalt und Anträge

I. Die Beschwerde der Anmelderin der europäischen Patentanmeldung Nr. 06020952.5 (Veröffentlichungsnummer EP 1 777 911 A) richtet sich gegen die Entscheidung der Prüfungsabteilung vom 5. Januar 2012, mit der die Anmeldung zurückgewiesen wurde.

Die Entscheidung wurde damit begründet, dass der Gegenstand des Anspruchs 9 des Hauptantrags sowie des Anspruchs 1 des vierten Hilfsantrags nicht erfinderisch sei (Artikel 52 (1) und 56 EPÜ) und dass die Ansprüche 1 und 9 des ersten, zweiten und dritten Hilfsantrags gegen das Erfordernis des Artikels 123 (2) EPÜ verstießen.

II. Das folgende Dokument, auf das in der angefochtenen Entscheidung Bezug genommen wurde, ist für die vorliegende Entscheidung relevant:

D1: EP 1 494 429 A.

III. Mit der Beschwerdebegründung beantragte die Beschwerdeführerin zumindest implizit die Aufhebung der angefochtenen Entscheidung und die Erteilung eines Patents auf der Grundlage der Ansprüche eines Hauptantrags, hilfsweise eines Hilfsantrags, jeweils mit der Beschwerdebegründung eingereicht.

IV. In einer der Ladung zur mündlichen Verhandlung beigefügten Mitteilung nahm die Kammer zum Sachverhalt vorläufig Stellung.

Dabei führte die Kammer unter Verweis auf Artikel 114 (1) EPÜ das folgende Dokument ein:

D3: US 2004/0193925 A.

V. In Erwiderung auf die Mitteilung der Kammer reichte die Beschwerdeführerin mit Schreiben vom 18. November 2016 einen geänderten Hilfsantrag ein.

VI. Am 19. Dezember 2016 fand eine mündliche Verhandlung vor der Beschwerdekammer statt.

Die Beschwerdeführerin nahm den Hauptantrag zurück und beantragte, als einzigen Antrag, die angefochtene Entscheidung aufzuheben und ein Patent auf der Grundlage der mit Schreiben vom 18. November 2016 als Hilfsantrag eingereichten Ansprüche zu erteilen.

Nach Schließen der Debatte und Beratung der Kammer verkündete der Vorsitzende die Entscheidung.

VII. Anspruch 1 des einzigen Antrags lautet:

"System zum Bereitstellen einer Kommunikation für einen in einem gesicherten Netzwerk (200) nicht eingebundenen Client-Computer (250) mit Ressourcen (201 bis 204) innerhalb des gesicherten Netzwerks, mit:
einem Client-Computer (250) mit mindestens einem Signaleingang (255),
einem transportablen, entnehmbaren, computerlesbaren Speichermedium (260), beinhaltend Authentifizierungsdaten (262), ein Verbindungsprogramm (264), und Einrichtungen (265), die dafür konfiguriert sind, das computerlesbare Speichermedium mit dem Client-Computer über den Signaleingang zu verbinden, wobei der Client-Computer kein installiertes Zertifikat zur Authentifizierung gegenueber dem Host-Computer (210) aufweist und stattdessen das Speichermedium die Authentifizierungsdaten und das Verbindungsprogramm

aufweist, wodurch es einem Besitzer des transportablen, entnehmbaren, computerlesbaren Speichermediums (260) möglich ist, von einem beliebigen Client-Computer (250) aus Kontakt zu dem gesicherten Netzwerk (200) aufzunehmen, und
einem Host-Computer (210), der mit dem gesicherten Netzwerk über eine gesicherte Verbindung verbunden ist, wobei der Client-Computer eingerichtet ist, wenn das computerlesbare Speichermedium mit dem Client-Computer über den Signaleingang verbunden ist, das Speichermedium als Datenspeicher zu erkennen, wodurch das Verbindungsprogramm auf dem Client-Computer automatisch gestartet und ausgeführt wird und das Verbindungsprogramm so konfiguriert ist, dass es bei Ausführung sicherstellt, dass der Client-Computer durch das Verbindungsprogramm (264) auf dem Speichermedium (260) unter Verwendung der Authentifizierungsdaten auf dem Speichermedium (260) eine sichere Verbindung zu dem Host-Computer herstellt, ,*[sic]* so dass der Host-Computer eine oder mehrere Anfragen des Client-Computers, die an Ressourcen innerhalb des gesicherten Netzwerks gerichtet sind, an das gesicherte Netzwerk weiterleitet,
und wobei die gesicherte Verbindung eine temporäre Verbindung zu dem gesicherten Netzwerk ist, die automatisch beendet wird, wenn der Besitzer des Speichermediums das Speichermedium aus dem Client-Computer entnimmt und diese Verbindung anschliessend von einem anderen Nutzer des Client-Computers ohne dem Speichermedium nicht mehr rekonstruiert werden kann, da der Client-Computer kein installiertes Zertifikat aufweist und die Authentifizierungsdaten auf dem Speichermedium gespeichert sind und somit bei dem Besitzer des Speichermediums verbleiben."

Entscheidungsgründe

1. *Anspruch 1 - Erfinderische Tätigkeit (Artikel 52 (1) und 56 EPÜ)*

1.1 D3 (s. Zusammenfassung) offenbart ein System mit einem tragbaren Kennwort-Management-Gerät mit zum Beispiel einer USB-Schnittstelle, das mit einem Client-Computer verbunden werden kann. Das tragbare Gerät ist so eingerichtet, dass vom Client-Computer aus eine Anmeldung bei Zielsystemen automatisch ausgeführt wird, ohne dass auf dem Client-Computer ein Programm konfiguriert oder installiert werden muss (Zusammenfassung).

Als Nachteil eines früheren Systems beschreibt die D3, dass bei ihm ein Programm auf dem Computer installiert werden müsse und Benutzer von öffentlich genutzten Computern wie beispielsweise in Flughäfen, Universitäten oder Internet-Cafes, für die sie keine Installationsrechte haben, keinen Zugang zu ihren Informationssystemen haben (Absatz [0004]).

Vor diesem Hintergrund wird in der D3 die Notwendigkeit für einen tragbaren, automatischen Kennwort-Manager beschrieben, der mit zahlreichen Client-Computern verwendet werden kann, ohne dass vorher auf ihnen eine Installation erforderlich ist (Absatz [0006]).

Dies wird gemäß der D3 erreicht, indem ein auf dem Kennwort-Manager gespeichertes Programm Anmeldeaufforderungen erkennt und automatisch die entsprechenden Zugangsdaten einträgt (Absatz [0023] und Anspruch 1).

1.2 Insbesondere offenbart D3 unter Verwendung der Begriffe aus Anspruch 1 ein System zum Bereitstellen einer

Kommunikation für einen in einem Zielsystem ("remote system") nicht eingebundenen Client-Computer ("host computer", Absatz [0018], Figure 1) mit dem Zielsystem, mit:
einem Client-Computer mit mindestens einem Signaleingang (der "Host-Computer" ist mit einem "portable device" verbindbar, was einen Signaleingang des "Host-Computer" impliziert, Beginn des Absatzes [0020]),
einem transportablen, entnehmbaren, computerlesbaren Speichermedium, beinhaltend Authentifizierungsdaten, ein Verbindungsprogramm und Einrichtungen, die dafür konfiguriert sind, das computerlesbare Speichermedium mit dem Client-Computer über den Signaleingang zu verbinden (das "portable device" weist "login information" und eine "software application component" auf, Absatz [0018], und kann ein USB-Speicher sein, der entnehmbar ist, Ende Absatz [0007]), und
einem Host-Computer (Teil des "remote system", bei dem sich der "host computer" identifiziert, Absatz [0018]),
wobei der Client-Computer kein installiertes Zertifikat zur Authentifizierung gegenueber dem Host-Computer aufweist (D3 offenbart kein installiertes Zertifikat auf dem "Host-Computer", Absatz [0006]) und stattdessen das Speichermedium die Authentifizierungsdaten und das Verbindungsprogramm aufweist, wodurch es einem Besitzer des transportablen, entnehmbaren, computerlesbaren Speichermediums möglich ist, von einem beliebigen Client-Computer ("any computer", Beginn Absatz [0020]) aus Kontakt zu dem Zielsystem aufzunehmen,
wobei der Client-Computer eingerichtet ist, wenn das computerlesbare Speichermedium mit dem Client-Computer über den Signaleingang verbunden ist, das Speichermedium als Datenspeicher zu erkennen, wodurch das Verbindungsprogramm auf dem Client-Computer automatisch gestartet und ausgeführt wird (Absatz

[0020], zweiter und dritter Satz, die automatische Ausführung impliziert zudem eine Erkennung als Datenspeicher) und das Verbindungsprogramm so konfiguriert ist, dass es bei Ausführung sicherstellt, dass der Client-Computer durch das Verbindungsprogramm auf dem Speichermedium unter Verwendung der Authentifizierungsdaten auf dem Speichermedium eine Verbindung zu dem Host-Computer herstellt (Absatz [0023] und Anspruch 1),
und wobei der Client-Computer kein installiertes Zertifikat aufweist und die Authentifizierungsdaten auf dem Speichermedium gespeichert sind und somit bei dem Besitzer des Speichermediums verbleiben.

1.3 Das beanspruchte System unterscheidet sich von dem aus der D3 bekannten dadurch, dass

a) das Zielsystem ein gesichertes Netzwerk mit darin liegenden Ressourcen ist und die bereitgestellte Kommunikation eine Kommunikation zwischen dem Client-Computer und den Ressourcen ist,

b) der Host Computer mit dem gesicherten Netzwerk über eine gesicherte Verbindung verbunden ist,

c) der Host-Computer eine oder mehrere Anfragen des Client-Computers, die an Ressourcen innerhalb des gesicherten Netzwerks gerichtet sind, an das gesicherte Netzwerk weiterleitet,

d) die Verbindung zwischen dem Client-Computer und dem Host-Computer eine sichere Verbindung ist, und

e) die gesicherte Verbindung eine temporäre Verbindung zu dem gesicherten Netzwerk ist, die automatisch beendet wird, wenn der Besitzer des Speichermediums das Speichermedium aus dem Client-Computer entnimmt und diese Verbindung anschließend von einem anderen Nutzer des Client-Computers ohne dem Speichermedium nicht mehr rekonstruiert werden kann.

1.4 Das System der D3 erlaubt es, sich mittels eines beliebigen Computers bei einem Zielsystem mittels Anmeldedaten anzumelden, ohne dass auf dem Computer ein Programm installiert werden müsste. Das Zielsystem ist nicht weiter beschrieben. Allerdings ist die Sicherheit einer Verbindung, die nur durch Anmeldung mit Anmeldedaten geschützt ist, vergleichsweise gering und in aller Regel nicht für sicherheitskritischere Anwendungen ausreichend, wie beispielsweise Zugriffe auf ein Firmennetzwerk.

1.5 Im Vergleich zu dem System der D3 verschaffen die Merkmal d) und e) eine erhöhte Sicherheit. Die Merkmale a) bis c) beschreiben Umstände, die bei einer Anwendung des Systems der D3 auf die Bereitstellung eines Fernzugangs in ein Firmennetzwerk mit seinen darin liegenden Ressourcen eintreten würden.

1.6 Die Kammer sieht daher die technische Aufgabe, die sich dem von D3 ausgehenden Fachmann stellt, darin, den Anwendungsbereich in Richtung sicherheitssensiblerer Anwendungen zu erweitern.

Da eine erhöhte Sicherheit ein grundsätzliches Bestreben ist, ebenso wie ein breiteres Anwendungsgebiet, kann die Formulierung dieser Aufgabe allein noch keinen Beitrag zur erfinderischen Tätigkeit leisten.

1.7 In Bezug auf die Sicherheit ist dem Fachmann bewusst, dass insbesondere die Übertragung der Daten zwischen dem Client-Computer und dem Host-Computer geschützt und das Speichermedium mit den Authentifizierungsdaten schützenswerte mögliche Angriffspunkte sind.

Die Verbindung gemäß Merkmal d) sicher zu machen, ist eine naheliegende Maßnahme, die im Rahmen des allgemeinen Fachwissen liegt. Diese Einschätzung gilt auch für eine als VPN-Verbindung ausgestaltete sichere Verbindung, die zum Prioritätszeitpunkt bereits aus der D1 bekannt war. Die Kammer verweist ferner auf das damals ebenfalls bekannte https(http secure)-Protokoll.

In Bezug auf die Authentifizierungsdaten war es naheliegend, dass die Sicherheit umso größer ist, je stärker die Benutzung der Authentifizierungsdaten für das Bereitstellen der Verbindung an den Besitz des Speichermediums geknüpft ist. Die D3 liefert in Absatz [0022] diesbezüglich auch bereits die Anregung, Vorkehrungen zum Detektieren von Sicherheitsauffälligkeiten beim Host-Computer vorzusehen. Unter die möglichen Sicherheits-auffälligkeiten gehört das Entfernen des Speichermediums vom Host-Computer, da andernfalls die Verbindung unabhängig vom Besitz des Speichermediums genutzt werden könnte. Als Reaktion auf das Entfernen des Speichermediums ist das Beenden der Verbindung die naheliegendste, da damit auf sehr einfache Weise ein möglicherweise unbefugter Zugang zum Host-Computer sicher verhindert wird. Eine starke Verknüpfung zwischen dem Speichermedium und der Benutzung der Verbindung zwischen dem Client-Computer und dem Host-Computer legt auch nahe, dass die Verbindung nach Entfernen des Speichermediums von anderen nicht rekonstruiert werden kann, da andernfalls die Verbindung unabhängig vom Besitz des Speichermediums genutzt werden könnte, was einer starken Verknüpfung zwischen dem Besitz des Speichermediums und der Verwendung der Authentifizierungsdaten zuwiderliefe.

Die Möglichkeit einer Beendigung wiederum impliziert, dass die Verbindung temporär ist. In diesem Zusammenhang merkt die Kammer an, dass es für sicherheitskritische Internet-Verbindungen, wie beispielsweise das Internet-Banking, bekannt war, die Verbindung nach einer bestimmten Zeit, in denen der Benutzer nicht aktiv war, zu unterbrechen.

Die Erhöhung der Sicherheit mittels der Merkmale d) und e) trägt somit nicht zu einer erfinderischen Tätigkeit bei.

Mit der Erhöhung der Sicherheit geht einher, dass die Anwendung des Systems gemäß D3 auch auf sicherheitskritische Gebiete wie beispielsweise das Bereitstellen eines Fernzugriffs auf ein Firmennetzwerk und seinen darin liegenden Ressourcen ausgeweitet werden kann. Dieser Anwendungsfall war zum Prioritätszeitpunkt der Anmeldung bekannt und beinhaltet weiterhin, da Firmennetzwerke als sicher angenommen werden können, dass der Host-Computer über eine sichere Verbindung mit dem sicheren Netzwerk als Zielsystem verbunden ist und an die Ressourcen gerichtete Anfragen an das sichere Netzwerk weiterleitet.

Somit tragen auch die Merkmale a) bis c) nicht zu einer erfinderischen Tätigkeit bei.

1.8 Die Beschwerdeführerin argumentierte, dass D3 nur eine Verbindung zwischen dem Client-Computer und dem Host-Computer offenbare, die mittels Benutzername und Kennwort geschützt und dies keine sichere Verbindung sei wie beispielsweise die in der Anmeldung erwähnte VPN-Verbindung. Weiter offenbare D3 zwar die Speicherung der Authentifizierungsdaten auf einem

tragbaren Speichermedium, ginge aber gerade nicht den weiteren Schritt, die Verbindung zwischen dem Client-Computer und dem Host-Computer sicher auszugestalten. Dies sei ein Indiz dafür, dass das System gemäß Anspruch 1 für einen von D3 ausgehenden Fachmann nicht nahegelegen habe.

Die Kammer folgt dem Argument nicht, da es zum Prioritätszeitpunkt der Anmeldung parallel unterschiedliche Anwendungen mit unterschiedlichen Sicherheitsanforderungen gab, wie beispielsweise der weniger sicherheitskritische Zugang zu einem Online-Versandhändler und der sicherheitskritischere Zugang zu einem Firmennetz. Der Fachmann würde flexibel die Sicherheitsmaßnahmen an die jeweiligen Anforderungen anpassen und die Verbindung zwischen dem Client-Computer und dem Host-Computer bei Bedarf sicher ausgestalten, ohne erfinderisch tätig zu werden. Daher kann die Tatsache, dass in dem System der D3 keine sichere Verbindung offenbart ist, nicht einen erfinderischen Beitrag durch eine Implementierung als sichere Verbindung stützen.

In diesem Zusammenhang verweist die Kammer auf die D1, die eine sichere VPN-Verbindung mit Zertifikat offenbart und aus der sich der Fachmann ebenfalls eine entsprechende Anregung hätte holen können, ohne erfinderische tätig werden zu müssen.

Daher beruht der beanspruchte Gegenstand nicht auf einer erfinderischen Tätigkeit (Artikel 56 EPÜ).

2. Da kein gewährbarer Antrag vorliegt, ist die Beschwerde zurückzuweisen.

Entscheidungsformel

Aus diesen Gründen wird entschieden:

Die Beschwerde wird zurückgewiesen.

Die Geschäftsstellenbeamtin: Der Vorsitzende:

G. Rauh F. van der Voort

Entscheidung elektronisch als authentisch bestätigt