(19) REPUBLIK ÖSTERREICH Patentamt

(10) Nummer: **AT 412 314 B**

(12) # PATENTSCHRIFT

(21) Anmeldenummer: A 455/2001
(22) Anmeldetag: 21.03.2001
(42) Beginn der Patentdauer: 15.05.2004
(45) Ausgabetag: 27.12.2004

(51) Int. Cl.[7]: **H04L 12/16**

(56) Entgegenhaltungen:
EP 0579338A1 JP 9293052A
EP 0952698A2 US 6131120A

(73) Patentinhaber:
SIEMENS AKTIENGESELLSCHAFT ÖSTERREICH
A-1210 WIEN (AT).

(72) Erfinder:
GRUBMAIR PETER
WIEN (AT).
ROHRER MARTIN
WIEN (AT).

(54) VERFAHREN UND VORRICHTUNG ZUM VERBINDEN EINES NACH DEM BLUETOOTH STANDARD ARBEITENDEN GERÄTES MIT EINEM DATENNETZ

(57) Es wird ein Verfahren zum Aufbau einer Verbindung zwischen einem ersten Gerät (DEV1) und einem Datennetz (NET) angegeben, wobei diese Verbindung über ein zweites Gerät (DEV2) im Datennetz (NET) hergestellt wird und mit Hilfe eines dritten Geräts (DEV3) die Zugriffsrechte auf Dienste (SERV) des Datennetzes (NET) für das erste Gerät (DEV1), sowie eine Liste jener Dienste (SERV), die auf einer Anzeigeeinheit des ersten Gerätes (DEV1) angezeigt werden sollen, ermittelt und an das zweite Gerät (DEV2) zurückgesendet werden. Die Kommunikation zwischen erstem Gerät (DEV1) und zweitem Gerät (DEV2) erfolgt dabei nach dem Bluetooth Standard. Weiterhin wird eine Anordnung zur Durchführung des Verfahrens angegeben.

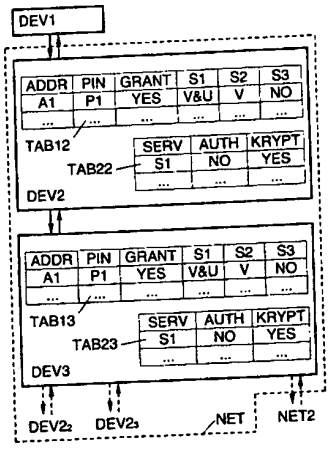

Fig.

AT 412 314 B

Die Erfindung betrifft ein Verfahren zum Aufbau einer Verbindung zwischen einem ersten Gerät und einem Datennetz, wobei

- diese Verbindung über ein zweites Gerät im Datennetz hergestellt wird und
- die Kommunikation zwischen erstem und zweitem Gerät nach dem Bluetooth Standard abgewickelt wird.

Weiterhin betrifft die Erfindung eine Anordnung zur Durchführung des erfindungsgemäßen Verfahrens.

In der jüngeren Vergangenheit wurden vermehrt Anstrengungen unternommen, die Kommunikation zwischen Geräten mittels Funkwellen über vergleichsweise kurze Distanzen zu standardisieren. Ein Resultat dieser Bemühungen ist der unter dem Begriff „Bluetooth" bekannte Standard, welcher die Nutzung des „2.4 GHz Industrial Scientific Medicine" Bandes, kurz 2.4 GHz ISM-Band, vorsieht und auf den gültigen Funkvorschriften für Europa, Japan und Nordamerika basiert. Die für den Standard relevanten Dokumente sind die „Specification of the Bluetooth System - Core v1.0B" vom 1 Dezember 1999 und die „Specification of the Bluetooth System - Profiles v1.0B" vom 1 Dezember 1999. Beide können unter der Internetadresse „http://www.bluetooth.com" erhalten werden.

Ein wesentliches Merkmal des erwähnten Standards ist die Art und Weise der Datenübertragung zwischen den Geräten. Einerseits besteht die Möglichkeit einen synchronen verbindungsorientierten Datenkanal, kurz SCO-Link, aufzubauen, andererseits kann auch ein asynchroner nicht verbindungsorientierter Datenkanal, kurz ACL-Link, geschaltet werden. Ein Gerät fungiert dabei als Master, die weiteren als Slaves, wobei die Geräte in einem Netzwerk zusammengefasst werden.

Der SCO-Link ist eine symmetrische Punkt-zu-Punkt Verbindung zwischen einem Master und einem einzigen Slave in einem Netzwerk. Der Master hält dabei den SCO-Link aufrecht indem regelmäßig reservierte Schlitze des Kanals verwendet werden. Typischerweise werden auf einem SCO-Link Sprachdaten übertragen. Vorraussetzung für den Aufbau einer solchen Datenverbindung ist ein bereits existierender ACL-Link.

Der ACL-Link ist eine Punkt zu Mehrpunkt Verbindung zwischen einem Master und allen Slaves des Netzwerkes und ermöglicht den paketvermittelten Datenverkehr zwischen den einzelnen Geräten. Zumeist wird dabei zwecks Datensicherung eine Rückmeldung an das sendende Gerät übermittelt.

Ein weiteres wesentliches Merkmal des Standards ist, dass zwischen den Geräten eines Netzwerkes stets eine bidirektionale Datenverbindung aufgebaut wird. Jedes Gerät umfasst daher immer eine Sende- und eine Empfangseinheit.

Ein Anwendungsfall für die Funkverbindung gemäß dem Bluetooth Standard ist in die Anbindung eines Gerätes, welches für die Kommunikation gemäß dem Bluetooth Standard geeignet ist, an ein Datennetz. Dieses Gerät kann beispielsweise ein Personal-Computers, ein Laptop, ein Personal Digital Assistant, kurz PDA, oder auch ein Mobiltelefon sein. Für das Datennetz kann zum Beispiel ein lokales Netzwerk, kurz LAN, wie es innerhalb von Betrieben häufig zu finden ist, oder aber auch das Internet vorgesehen sein.

Der Zugang zum Datennetz wird dabei in der Regel mit Hilfe eines speziellen Gerätes bewerkstelligt, das einerseits für die Kommunikation gemäß dem Bluetooth Standard geeignet ist, andererseits aber auch die Einbindung in eine Datennetz ermöglicht.

Nach dem Bluetooth-Standard wird der Aufbau einer Verbindung eines Gerätes in ein LAN folgendermaßen realisiert:

Zu Beginn wird vom Benutzer des Bluetooth-fähigen Gerätes ein sogenannter LAN Access Point, kurz LAP, ausgewählt, der sich innerhalb seines Empfangsbereichs befindet. Dieser LAP muss für die Kommunikation gemäß dem Point to Point Protocol, kurz PPP, dem Logical Link Control and Adaption Protocol, kurz L2CAP, und dem Serial Cable Emulation Protocol, kurz RFCOMM, geeignet sein.

Danach wird eine Verbindung zwischen dem Bluetooth-fähigen Gerät und dem LAP aufgebaut und in Folge eine PPP/RFCOMM/L2CAP-Verbindung hergestellt. Für die Authentifizierung kann auch die Abfrage eines Benutzernamens und eines Passworts vorgesehen sein. Erst wenn diese korrekt übermittelt wurden, bleibt die Verbindung dauerhaft bestehen.

Eine Authentifizierung nach dem PPP-Protocol ist dabei unabhängig von der Authentifizierung nach dem Bluetooth-Standard. Denkbar ist daher auch die Kombination dieser beiden Mechanis-

men.

Zwischen dem LAP und dem Gerät wird dann eine Adresse gemäß dem Internet Protocol, kurz IP-Adresse, vereinbart. Der Benutzer des Bluetooth-fähigen Geräts kann nun die Dienste des Datennetzes nutzen.

Da es in der Regel nicht erwünscht sein wird, dass jeder Dienst für jedermann zugänglich ist, müssen entsprechende Zugriffsberechtigungen verteilt werden. Versucht ein Benutzer einen Dienst in Anspruch zu nehmen, für den er kein Zugriffsrecht erhalten hat, so wird diese Anforderung abgewiesen.

Aus dem Stand der Technik sind hierzu einige Möglichkeiten bekannt:

Aus der EP 0 579 338 A1, „Verfahren und Einrichtung zur Zugriffsüberwachung und zum Zugriffsschutz in Kommunikationsnetzwerken", vom 18. November 1993 ist beispielsweise bekannt, dass der gesamte Datenverkehr in einem Netzwerk durch eine zentrale Überwachungseinrichtung abgehört wird und Telegramme einer bestimmten Art unwirksam gemacht werden. Die Datensicherung erfolgt dabei auf der „Grundlage des Vertrauens", das heißt der Datenverkehr wird prinzipiell zugelassen und lediglich im Einzelfall nachträglich unterbunden. Nachteilig an diesem Verfahren ist, dass dies zu unnötigem Datenverkehr führt und dass eine zentrale Überwachung insbesondere bei großen, verteilten Netzwerken schwierig durchzuführen ist.

Die Schrift JP 9 293 052 A, „Method and system for authorization management between plural networks", vom 11. November 1997 offenbart weiters eine Sicherungseinrichtung zwischen zwei Netzwerken. Auch hier wird eine Dienstanforderung prinzipiell zugelassen und allenfalls an einer Netzwerkgrenze abgewiesen, was auch hier zu erhöhtem Datenverkehr führt.

Weiters wird in der EP 0 952 698 A2, „System and method for restricting database access to managed object information using a permissons table", vom 27. Oktober 1999 eine Zugriffssicherung zu Objekten einer Datenbank mit Hilfe einer Berechtigungstabelle bekannt. Dabei erteilt ein Zutrittskontrollsystem den Nutzern eine Zutrittsberechtigung anhand von den in einer Zutrittskontrolldatenbank spezifizierten Rechten. Diese Rechte definieren die Berechtigung bestimmter Benutzer oder Benutzergruppen, auf einen bestimmten Satz von verwalteten Objekten zuzugreifen. Da eine etwaige Berechtigung hier erst beim Zugriff auf ein Objekt selbst erteilt wird, kommt es auch bei diesem Verfahren zu unnötigem Datenverkehr.

Schließlich wird in der Druckschrift US 6 131 120 A, „Enterprise network management directory containing network addresses of users and devices providing access lists to routers and servers", vom 10. Oktober 2000 ein Netzwerkverwaltungsverzeichnis offengelegt, welches Netzwerkadressen von Benutzern und Geräten enthält und Zutrittslisten für Router und Server verfügbar macht.

Nach dem Stand der Technik ist es für den Benutzer also im Normalfall erst dann erkennbar ob er einen Dienst benutzen kann oder nicht, nachdem er diesen Dienst angefordert hat.

Diese Art der Erteilung eines Zugangs zu einem Dienst eines Datennetzes ist unkomfortabel und ineffizient, da in das Datennetz eine Vielzahl von Anfragen über den Zugang übermittelt werden müssen.

Aufgabe der Erfindung ist es daher den Zugang zu Diensten eines Datennetzes mittels Geräten, welche zur Kommunikation nach dem Bluetooth Standard geeignet sind, auf vergleichsweise einfache Weise zu ermöglichen.

Dies geschieht erfindungsgemäß mit einem Verfahren der eingangs genannten Art,

- bei dem das zweite Gerät vor dem Aufbau der Verbindung zwischen erstem Gerät und dem Datennetz eine Anforderung zur Vergabe von Zugriffsrechten zu einem dritten Gerät im Datennetz sendet,
- bei dem mittels drittem Gerät Zugriffsrechte für das erste Gerät, sowie eine Liste jener Dienste, die auf einer Anzeigeeinheit des ersten Gerätes angezeigt werden sollen, ermittelt und an das zweite Gerät zurückgesendet werden,
- bei dem mit Hilfe dieser Zugriffsrechte der Zugang zu zumindest einem Teil der Dienste des Datennetzes für das erste Gerät geregelt wird und
- bei dem die Liste anzuzeigender Dienste zum ersten Gerät weitergeleitet wird und dort auf einer Anzeigeeinheit angezeigt wird.

Unter Diensten eines Datennetzes können sämtliche Dienste des Internets und innerbetrieblicher Netze, auch bekannt unter dem Begriff „Intranet", verstanden werden. Darüber hinaus sind noch weitere Dienste denkbar, bei denen Geräte, welche einen Dienst zur Verfügung stellen, in ein

Datennetz eingebunden sind.

Dazu gehören unter anderem Systeme in der Haustechnik, beispielsweise zur Steuerung von Rollladen, Jalousien, Fensteröffnern, Alarmanlagen und Garagentoren, sowie Systeme in der Unterhaltungselektronik, zum Beispiel zur Steuerung von Fernsehern, Audiogeräten, Spielzeugen und dergleichen. Des weiteren finden sich auch in der industriellen Umgebung zahlreiche Beispiele, wie etwa Systeme zur Steuerung von Kränen, Beleuchtung, Maschinen und Fahrzeugen. In der Büro-Umgebung können Geräte, wie zum Beispiel Drucker, Scanner und dergleichen angesteuert werden.

Die erwähnten Beispiele sind keinesfalls als vollständige Aufzählung der möglichen Anwendungsfälle zu verstehen und sollen nur dazu dienen, den großen Anwendungsbereich dieser Systeme aufzuzeigen.

Für die Anforderung zur Vergabe von Zugriffsrechten wird beispielsweise die entsprechende Adresse des ersten Geräts an das dritte Gerät übermittelt. Dort können die entsprechenden Zugriffsrechte, zum Beispiel unter Verwendung einer Tabelle, in der jeder Geräteadresse ein bestimmter Umfang von Diensten zugeordnet wird, leicht ermittelt werden. Ist für die entsprechende Geräteadresse kein Eintrag vorhanden, weil das zugehörige erste Gerät noch nicht registriert wurde, so können auch standardmäßige Zugriffsrechte für verschiedene Dienste erteilt werden. Für diesen Zweck kann in der Tabelle ein sogenannter „Dummy-Eintrag" vorgesehen sein, der immer dann ausgewählt wird, wenn sich für die übermittelte Adresse kein spezifischer Eintrag ermitteln lässt.

Den einzelnen Diensten können wiederum weitere Parameter zugeordnet werden, beispielsweise welches Protokoll für die Nutzung eines Dienstes verwendet werden soll, zeitliche Beschränkungen für die Nutzung eines Dienstes und dergleichen.

Die entsprechenden Tabellen im dritten Gerät können durch die Einbindung des dritten Gerätes in ein Datennetz auf vergleichsweise einfache Weise verwaltet werden. Denkbar ist dabei eine für das Internet gebräuchliche Schnittstelle über einen sogenannten „Webbrowser". Der Verwendung von Tabellen zur Erteilung von Zugriffsrechten ist aber nicht zwingend, sondern stellt nur eine von vielen möglichen Ausgestaltungen dar.

Vorteilhaft an der Erfindung ist auch, dass der Benutzer des ersten Gerätes überhaupt nur aus jenen Diensten auswählen kann, für die er auch das Zugangsrecht erhalten hat. Für den Benutzer wird die Nutzung der Dienste eines Datennetzes daher wesentlich vereinfacht. Es wird in der Regel daher nicht vorkommen, dass der Zugang zu einem Dienst erst nach dessen Anforderung abgewiesen wird, es sei denn, dass der Dienst noch über eine zusätzliche Absicherung verfügt. Diese Sicherung kann bei besonders kritischen Diensten im Bezug auf die Sicherheit, aber auch beispielsweise bei der Nutzung von kostenpflichtigen Diensten vorgesehen sein. In letzterem Fall ist die Angabe einer Kreditkartennummer, einer Bankverbindung oder eines auf einer Wertkarte enthaltenen Codes denkbar.

Günstig ist es, wenn die Verbindung zwischen erstem Gerät und dem Datennetz nur dann hergestellt wird, wenn das Zugriffsrecht dafür erteilt wurde. Somit werden Ressourcen geschont, da nur jene Geräte in das Datennetz eingebunden werden, mit denen die Nutzung zumindest eines Dienstes des Datennetzes potentiell möglich ist. Darüber hinaus ist es unter Berücksichtigung sicherheitsrelevanter Aspekte günstiger, Geräte, für die aus bestimmten Gründen ein Zugang zu den Diensten eines Datennetzes nicht vorgesehen ist, überhaupt nicht mit dem Datennetz zu verbinden.

Vorteilhaft ist es auch,

- wenn mittels drittem Gerät ein dem ersten Gerät zugeordneter Zugangscode ermittelt und an das zweite Gerät zurückgesendet wird und
- wenn der Zugriff auf bestimmte Dienste des Datennetzes nur gewährt wird, wenn der Zugangscode mittels erstem Gerät an das zweite Gerät übermittelt wird.

Für diese Variante kann im dritten Gerät eine Tabelle verwaltet werden, in der jeder Adresse eines ersten Geräts ein Zugangscode, beispielsweise eine Personal Identification Number, kurz PIN, zugeordnet ist. Mittels dieser Tabelle kann der Zugangscode im dritten Gerät vergleichsweise einfach ermittelt und an das zweite Gerät zurückgeschickt werden. Neben der Geräteadresse stellt dieser Zugangscode eine weitere Möglichkeit zur Absicherung von Diensten eines Datennetzes dar. Dabei kann die Verbindung zwischen erstem Gerät und Datennetz an sich von der Übermitt-

lung eines korrekten Zugangscodes abhängig gemacht werden. Denkbar ist auch, dass der Zugang verwehrt wird, wenn der Zugangscode mehrmals falsch eingegeben wurde.

Besonders vorteilhaft ist es weiterhin, wenn die vom dritten Gerät aufgrund einer Anforderung ermittelten Daten zumindest teilweise im zweiten Gerät zwischengespeichert werden. Dies ist eine sehr effiziente Ausgestaltung der Erfindung, da die Anfragen an das dritte Gerät auf diese Weise minimiert werden und darüber hinaus die für die Kommunikation zwischen erstem und zweitem Gerät relevanten Daten nach der ersten Abfrage wesentlich schneller verfügbar sind, als dies bei einer neuerlichen Abfrage beim dritten Gerät möglich wäre.

Eine besonders vorteilhafte Ausgestaltung der Erfindung ist auch gegeben, wenn die zwischengespeicherten Daten nach einer vorgebbaren Zeit verworfen werden. Da die Verbindung des ersten Gerätes in das Datennetz in der Regel nur über eine vergleichsweise kurze Zeitspanne genützt wird, also vom Wesen her eine temporäre Verbindung darstellt, werden die zwischengespeicherten Daten nach einer vorgebbaren Zeit verworfen. Diese Zeitspanne kann dabei vom Beginn der Verbindung an gerechnet werden, zum Beispiel eine Stunde ab Beginn der Verbindung, bis zu einem bestimmten Zeitpunkt, beispielsweise bis 24:00, oder von einem bestimmten Ereignis weg, zum Beispiel 5 Minuten seit der letzten Eingabe. Bei der Bemessung der Zeitspanne können auch sicherheitsrelevante Aspekte berücksichtigt werden, damit der Zugang zu einem Datennetz nicht auf unbestimmte Zeit möglich ist. Weiterhin wird so auch auf vergleichsweise einfache Weise vermieden, dass auf dem zweiten und dritten Gerät unterschiedliche Daten verwaltet werden. Andernfalls können die Daten auf dem zweiten und dritten Gerät auch durch regelmäßiges Abgleichen konsistent gehalten werden.

Die erfindungsgemäße Aufgabe wird auch gelöst durch eine Anordnung zur Durchführung des erfindungsgemäßen Verfahrens,

- bei der ein Datennetz ein zweites Gerät und ein drittes Gerät umfasst,
- bei der das zweite Gerät als Zugangspunkt für ein erstes Gerät zu diesem Datennetz vorgesehen ist,
- bei der das erste und das zweite Gerät und für die Kommunikation nach dem Bluetooth-Standard ausgerüstet sind,
- bei der das dritte Gerät für die Vergabe von Zugriffsrechten für den Zugang zu zumindest einem Teil der Dienste des Datennetzes für das erste Gerät, sowie für die Ermittlung einer Liste jener Dienste, die auf einer Anzeigeeinheit des ersten Gerätes angezeigt werden sollen, geeignet ist und
- bei der das dritte Gerät für das Senden und das zweite Gerät für das Empfangen dieser Zugriffsrechte und dieser Liste geeignet ist.

Vorteilhaft wird so die Möglichkeit geschaffen, dass ein drittes Gerät in einem Datennetz für die Vergabe von Zugriffsrechten an mehrere zweite Geräte vorgesehen ist. Die zweiten Geräte können so vergleichsweise einfach aufgebaut werden, da die Vergabe zentral erfolgt.

Mit der erfindungsgemäßen Anordnung werden auch die Voraussetzungen für eine komfortable Nutzung der Dienste eines Datennetzes durch den Benutzer des ersten Gerätes geschaffen. Die Anforderung eines Dienstes kann bei mangelndem Zugriffsrecht so nämlich schon im vorhinein abgewiesen werden.

Günstig ist es,

- wenn das dritte Gerät für die Ermittlung eines dem ersten Gerät zugeordneten Zugangscodes geeignet ist und
- wenn das dritte Gerät für das Senden und das zweite Gerät für das Empfangen dieses Zugangscodes geeignet ist.

Diese Variante der Erfindung kann vorteilhaft eingesetzt werden, wenn eine bessere Absicherung der Dienste eines Datennetzes erwünscht ist. Dabei ist beispielsweise in einer Tabelle im dritten Gerät jeder registrierten Geräteadresse ein Zugangscode zugeordnet.

Eine besonders vorteilhafte Ausgestaltung der Erfindung ist bei einer Anordnung gegeben, bei der das zweite Gerät Mittel zur Speicherung der vom dritten Gerät aufgrund einer Anforderung ermittelten Daten umfasst. Auf diese Weise können die Anfragen an das dritte Gerät wesentlich reduziert werden, da das zweite Gerät gegebenenfalls auf die intern gespeicherten Daten zurückgreifen kann.

Günstig ist dabei auch, wenn das zweite Gerät Mittel für das Verwerfen dieser Daten nach

einer vorgebbaren Zeit umfasst.

Dies ist eine ressourcenschonende Variante der Erfindung, da die zwischengespeicherten Daten nicht auf unbestimmte Zeit im zweiten Gerät verwaltet werden müssen. Darüber hinaus wird so auch vermieden, dass im zweiten und dritten Gerät unterschiedliche Daten gespeichert sind.

Es wird darauf hingewiesen das die für das erfindungsgemäße Verfahren angeführten Vorteile auch sinngemäß für die erfindungsgemäße Anordnung gelten.

Die Erfindung wird anhand einer Figur näher erläutert, welche eine beispielhafte Anordnung zur Durchführung des erfindungsgemäßen Verfahrens zeigt.

Die Figur umfasst ein erstes Gerät DEV1, ein zweites Gerät DEV2 und ein drittes Gerät DEV3, wobei das erste Gerät DEV1 mit dem zweiten Gerät DEV2 über eine Funkverbindung gemäß dem Bluetooth-Standard und das zweite Gerät DEV2 mit dem dritten Gerät DEV3 über eine bidirektionale Datenleitung, verbunden ist. Optional kann das dritte Gerät DEV3 mit einem zweiten zweiten Gerät DEV22 und einem dritten zweiten Gerät DEV23 verbunden sein. Das zweite Gerät DEV2, das dritte Gerät DEV3, das zweite zweite Gerät DEV22 und das dritte zweite Gerät DEV23 sind Bestandteil eines Datennetzes NET. Zusätzlich kann das dritte Gerät DEV3 mit einem zweiten Datennetz NET2 verbunden sein. Unter Datenleitungen sind in diesem Zusammenhang auch Funkverbindungen zu verstehen, beispielsweise Richtfunkstrecken.

Das dritte Gerät DEV3 umfasst in diesem Beispiel eine erste Tabelle TAB13, wobei in der ersten Spalte die Geräteadresse ADDR in der zweiten Spalte der Zugangscode PIN, in der dritten Spalte das Zugriffrecht zum Datennetz GRANT, in der vierten, fünften und sechsten Spalte das Zugriffsrecht zu einem ersten Dienst S1, einem zweiten Dienst S2 und einem dritten Dienst S3 eingetragen ist. Der leichteren Verständlichkeit halber werden in der Figur nicht mehr als drei Dienste dargestellt.

Jedes erste Gerät DEV1, das registriert wurde, wird durch eine Zeile repräsentiert. Im gezeigten Beispiel ist in der ersten Zeile die Geräteadresse A1, der Zugangscode P1, für das Zugriffsrecht zum Datennetz YES, für das Zugriffsrecht zum ersten Dienst V&U, für das Zugriffsrecht zum zweiten Dienst V und für das Zugriffsrecht auf den dritten Dienst NO eingetragen. Der leichteren Verständlichkeit halber wird in der Figur nur eine Zeile dargestellt, alle weiteren durch Punkte symbolisiert. Eine Zeile kann dabei auch einer Gruppe von ersten Geräten DEV1 zugeordnet werden. Ein Spezialfall ist die Zuordnung zu allen ersten Geräten DEV1, die nicht durch eine eingetragene Geräteadresse ADDR repräsentiert werden. Für diesen Spezialfall ist auch der Begriff „Dummy" gebräuchlich.

Weiterhin umfasst das dritte Gerät DEV3 eine zweite Tabelle TAB23, wobei in die erste Spalte der Name eines Dienstes SERV, in die zweite Spalte die Authentifizierung AUTH und die dritte Spalte die Verschlüsselung KRYPT eingetragen wird.

Jeder Dienst des Datennetzes NET wird durch eine Zeile repräsentiert. Im gezeigten Beispiel ist in der ersten Zeile der Name des Dienstes S1, für die Authentifizierung NO und für die Verschlüsselung YES eingetragen. Der leichteren Verständlichkeit halber wird auch in dieser Tabelle nur eine Zeile dargestellt, alle weiteren durch Punkte symbolisiert. Eine Zeile kann dabei auch einer Gruppe von Diensten zugeordnet werden. Ein Spezialfall ist auch hier die Zuordnung zu allen Diensten, die nicht durch einen eingetragenen Namen SERV repräsentiert werden.

Das zweite Gerät DEV2 ist im Beispiel hinsichtlich der ersten Tabelle TAB12 und der zweiten Tabelle TAB22 identisch mit dem dritten Gerät DEV3 aufgebaut. Diese Vereinfachung wurde vorgenommen um das Beispiel übersichtlich zu gestalten. Keinesfalls ist dieser Umstand zwingend erforderlich. Gegebenenfalls kann eine Tabelle im zweiten Gerät DEV2 überhaupt fehlen.

An dieser Stelle wird auch darauf hingewiesen, dass der Aufbau des zweiten Gerätes DEV2 und des dritten Gerätes DEV3 lediglich beispielhaft zu sehen ist. Auch der Aufbau und Inhalt der ersten Tabelle TAB1 und der zweiten Tabelle TAB2 ist nicht zwingend und dient lediglich der Veranschaulichung der Erfindung.

Die Funktion der in der Figur gezeigten Anordnung ist wie folgt:

Während eines Initialisierungsvorgangs werden die erforderlichen Daten, beispielsweise von einem Netzwerkadministrator, im dritten Gerät DEV3 gespeichert.

Der Eintrag in der ersten Zeile in der ersten Tabelle TAB13 ist dabei einem Gerät mit Geräteadresse A1 und dem Zugriffscode P1 zugeordnet. Für dieses Gerät wird das Zugriffsrecht auf das Datennetz NET durch den Eintrag YES in die Spalte GRANT erteilt, andernfalls wäre NO einzutra-

gen. Der erste Dienst S1 soll auf dem ersten Gerät DEV1 angezeigt werden. Zusätzlich wird der Zugriff auf diesen Dienst gewährt. In die Spalte S2 wird daher V für sichtbar oder „visible" und U für nutzbar oder „usable", also V&U eingetragen. Der zweite Dienst S2 soll nur beim ersten Gerät DEV1 angezeigt werden aber nicht unmittelbar nutzbar sein, weil vorher beispielsweise noch die Eingabe eines zusätzlichen Codes oder einer Kreditkartennummer erforderlich ist. Der Eintrag in die Spalte S2 lautet daher lediglich V. Das Zugriffsrecht für den dritten Dienst S3 soll nicht gewährt werden, weswegen in die Spalte S3 der Wert NO eingetragen wird.

In die zweite Tabelle TAB23 werden ebenfalls während eines Initialisierungsvorganges die einzelnen Dienste eingetragen. Beispielhaft wird in die erste Spalte SERV für den ersten Dienst S1 eingetragen.

Eine Authentifizierung bei der Nutzung dieses Dienstes soll nicht erforderlich sein, weswegen in die Spalte AUTH der Wert NO eingetragen wird. Andernfalls müsste der Wert YES eingetragen werden. Für die Verschlüsselung wird in die Spalte KRYPT der Wert YES eingetragen. Der Initialisierungsvorgang ist damit im gezeigten Beispiel abgeschlossen.

Vereinfachend wird angenommen, dass die erste Tabelle TAB12 im zweiten Gerät DEV2 zu diesem Zeitpunkt noch leer ist und die zweite Tabelle TAB22 des zweiten Geräts DEV2 identisch mit der zweiten Tabelle TAB23 des dritten Geräts DEV3 ist. Der Abgleich der beiden zweiten Tabellen TAB22 und TAB33 kann dabei beispielsweise in regelmäßigen Abständen erfolgen.

Soll nun zwischen erstem Gerät DEV1 und dem Datennetz NET eine Verbindung aufgebaut werden, wird mittels zweitem Gerät DEV2 vor dem Aufbau der endgültigen Verbindung eine Anforderung zur Vergabe von Zugriffsrechten zum dritten Gerät DEV3 gesendet. Zusätzlich wird dabei die Geräteadresse des ersten Gerätes DEV1 übermittelt. Im gezeigten Beispiel soll diese Adresse A1 lauten.

Der Aufbau der Verbindung zwischen erstem Gerät DEV1 und dem Datennetz NET ist unabhängig von einer bestehende Verbindung zwischen erstem und zweiten Gerät DEV1 und DEV2 nach dem Bluetooth-Standard. Letztere ist selbstverständlich nötig um überhaupt eine Anfrage vom ersten Gerät DEV1 an das zweite Gerät DEV2 zu richten und bildet die Grundlage für eine Verbindung in das Datennetz (NET), ist aber nicht mit der eigentlichen Verbindung in das Datennetz (NET) gleichzusetzen.

Mittels drittem Gerät DEV3 und erster Tabelle TAB13 werden nun die Zugriffsrechte für die Dienste ermittelt. Dabei wird die erste Zeile in der ersten Tabelle TAB13 als maßgebend erkannt und an das zweite Gerät DEV2 zurückgesendet. Im der ersten Tabelle TAB12 des zweiten Geräts DEV2 wird eine Kopie dieser Zeile zwischengespeichert und der Zugriff auf das Datennetz NET erteilt, da in der Spalte GRANT für die Geräteadresse A1 der Wert YES eingetragen ist. Andernfalls würde die Zeile verworfen und die Verbindung zum ersten Gerät DEV1 nicht gestattet werden.

In der Folge wird, in der Regel automatisch, eine Anfrage vom ersten Gerät DEV1 an das zweite Gerät DEV2 gesendet, welche Dienste nun zur Verfügung stehen. Mittels zweitem Gerät DEV2 und der ersten Tabelle TAB12 wird nun ermittelt, für welche Dienste das Zugriffsrecht erteilt wurde. Im gezeigten Beispiel wird also eine Liste an das erste Gerät DEV1 gesendet, die den ersten Dienst S1 und den zweiten Dienst S2 beinhaltet. Da in der ersten Tabelle TAB12 für beide Dienste der Wert V eingetragen wurde, werden diese auch beim ersten Gerät DEV1 angezeigt.

Der Benutzer des ersten Gerätes DEV1 kann nun aus dieser Liste auswählen und eine Anforderung zum Start eines Dienstes an das zweite Gerät DEV2 stellen. Der Zugriff auf den ersten Dienst S1 wird mittels zweitem Gerät DEV2 unmittelbar gewährt, da in der ersten Tabelle TAB12 für diesen Dienst neben dem Wert V auch der Wert U, also V&U eingetragen wurde.

Für die Nutzung des zweiten Dienstes S2 ist dagegen im gezeigten Beispiel noch die Angabe einer weiteren Zugangsberechtigung erforderlich, da in der ersten Tabelle TAB12 für diesen Dienst lediglich der Wert V eingetragen wurde.

Es wird darauf hingewiesen, dass unabhängig von der Erteilung eines Zugriffsrechts auf einen bestimmten Dienst durch das zweite Gerät DEV2 noch weitere Beschränkungen im Zugang zu diesem Dienst bestehen können. Ein Beispiel wäre, wenn etwa der prinzipielle Zugang zum Internet mittels zweitem Gerät DEV2 gewährt wird, ein bestimmter Dienst im Internet aber nur mit Hilfe eines Zugangscodes ausgeführt werden kann.

Mittels zweiter Tabelle TAB22 und zweitem Gerät DEV2 wird weiterhin bestimmt, wie die Nutzung eines Dienstes erfolgen soll. Im gezeigten Beispiel wird für die Nutzung des ersten Dienstes

S1 keine Authentifizierung verlangt, da in der zweiten Tabelle TAB22 des zweiten Geräts DEV2 in der Spalte AUTH der Wert NO eingetragen wurde. Weiterhin erfolgt die Datenübertragung unverschlüsselt, da in der zweiten Tabelle TAB22 des zweiten Geräts DEV2 in der Spalte KRYPT der Wert YES eingetragen wurde.

Der Eintrag für die Geräteadresse A1 in der ersten Tabelle TAB12 des zweiten Gerätes DEV2 wird in der Regel nach einer bestimmten Zeit verworfen, um nicht unnötig Ressourcen zu belegen und die nötige Sicherheit beim Zugriff auf das Datennetz NET zu gewähren. Möchte der Benutzer des ersten Gerätes DEV1 nochmals eine Verbindung zum Datennetz NET herstellen, muss das angeführte Verfahren nochmals ausgeführt werden.

PATENTANSPRÜCHE:

1. Verfahren zum Aufbau einer Verbindung zwischen einem ersten Gerät und einem Datennetz, wobei
   - diese Verbindung über ein zweites Gerät im Datennetz hergestellt wird und
   - die Kommunikation zwischen erstem und zweitem Gerät nach dem Bluetooth Standard abgewickelt wird,

   dadurch gekennzeichnet,
   - dass das zweite Gerät (DEV2) vor dem Aufbau der Verbindung zwischen erstem Gerät (DEV1) und dem Datennetz (NET) eine Anforderung zur Vergabe von Zugriffsrechten zu einem dritten Gerät (DEV3) im Datennetz (NET) sendet,
   - dass mittels drittem Gerät (DEV3) Zugriffsrechte für das erste Gerät (DEV1), sowie eine Liste jener Dienste (SERV), die auf einer Anzeigeeinheit des ersten Gerätes (DEV1) angezeigt werden sollen, ermittelt und an das zweite Gerät (DEV2) zurückgesendet werden,
   - dass mit Hilfe dieser Zugriffsrechte der Zugang zu zumindest einem Teil der Dienste (SERV) des Datennetzes (NET) für das erste Gerät (DEV1) geregelt wird und
   - dass die Liste anzuzeigender Dienste zum ersten Gerät (DEV1) weitergeleitet wird und dort auf einer Anzeigeeinheit angezeigt wird.
2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet,** dass die Verbindung zwischen erstem Gerät (DEV1) und dem Datennetz (NET) nur dann hergestellt wird, wenn das Zugriffsrecht dafür erteilt wurde.
3. Verfahren nach einem der Ansprüche 1 bis 2, **dadurch gekennzeichnet,**
   - dass mittels drittem Gerät (DEV3) ein dem ersten Gerät (DEV1) zugeordneter Zugangscode (PIN) ermittelt und an das zweite Gerät (DEV2) zurückgesendet wird und
   - dass der Zugriff auf bestimmte Dienste (SERV) des Datennetzes (NET) nur gewährt wird, wenn der Zugangscode (PIN) mittels erstem Gerät (DEV1) an das zweite Gerät (DEV2) übermittelt wird.
4. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet,** dass die vom dritten Gerät (DEV3) aufgrund einer Anforderung ermittelten Daten zumindest teilweise im zweiten Gerät (DEV2) zwischengespeichert werden.
5. Verfahren nach Anspruch 4, **dadurch gekennzeichnet,** dass die zwischengespeicherten Daten nach einer vorgebbaren Zeit verworfen werden.
6. Anordnung zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet,**
   - dass Datennetz (NET) ein zweites Gerät (DEV2) und ein drittes Gerät (DEV3) umfasst,
   - dass das zweite Gerät (DEV2) als Zugangspunkt für erstes Gerät (DEV1) zu diesem Datennetz (NET) vorgesehen ist,
   - dass das erste und das zweite Gerät (DEV1) und (DEV2) für die Kommunikation nach dem Bluetooth-Standard ausgerüstet sind,
   - dass das dritte Gerät (DEV3) für die Vergabe von Zugriffsrechten für den Zugang zu zumindest einem Teil der Dienste (SERV) des Datennetzes (NET) für das erste Gerät (DEV1), sowie für die Ermittlung einer Liste jener Dienste (SERV), die auf einer Anzeigeeinheit des ersten Gerätes (DEV1) angezeigt werden sollen, geeignet ist und

- dass das dritte Gerät (DEV3) für das Senden und das zweite Gerät (DEV2) für das Empfangen dieser Zugriffsrechte und dieser Liste geeignet ist.

7. Anordnung nach Anspruch 6, **dadurch gekennzeichnet,**
   - dass das dritte Gerät (DEV3) für die Ermittlung eines dem ersten Gerät (DEV1) zugeordneten Zugangscodes (PIN) geeignet ist und
   - dass das dritte Gerät (DEV3) für das Senden und das zweite Gerät (DEV2) für das Empfangen dieses Zugangscodes (PIN) geeignet ist.
8. Anordnung nach einem der Ansprüche 6 bis 7, **dadurch gekennzeichnet**, dass das zweite Gerät (DEV2) Mittel zur Speicherung der vom dritten Gerät (DEV3) aufgrund einer Anforderung ermittelten Daten umfasst.

HIEZU 1 BLATT ZEICHNUNGEN

ÖSTERREICHISCHES PATENTAMT
Ausgegeben am: 27.12.2004
Blatt: 1

Patentschrift Nr.: AT 412 314 B
Int. Cl. [7]: H04L 12/16

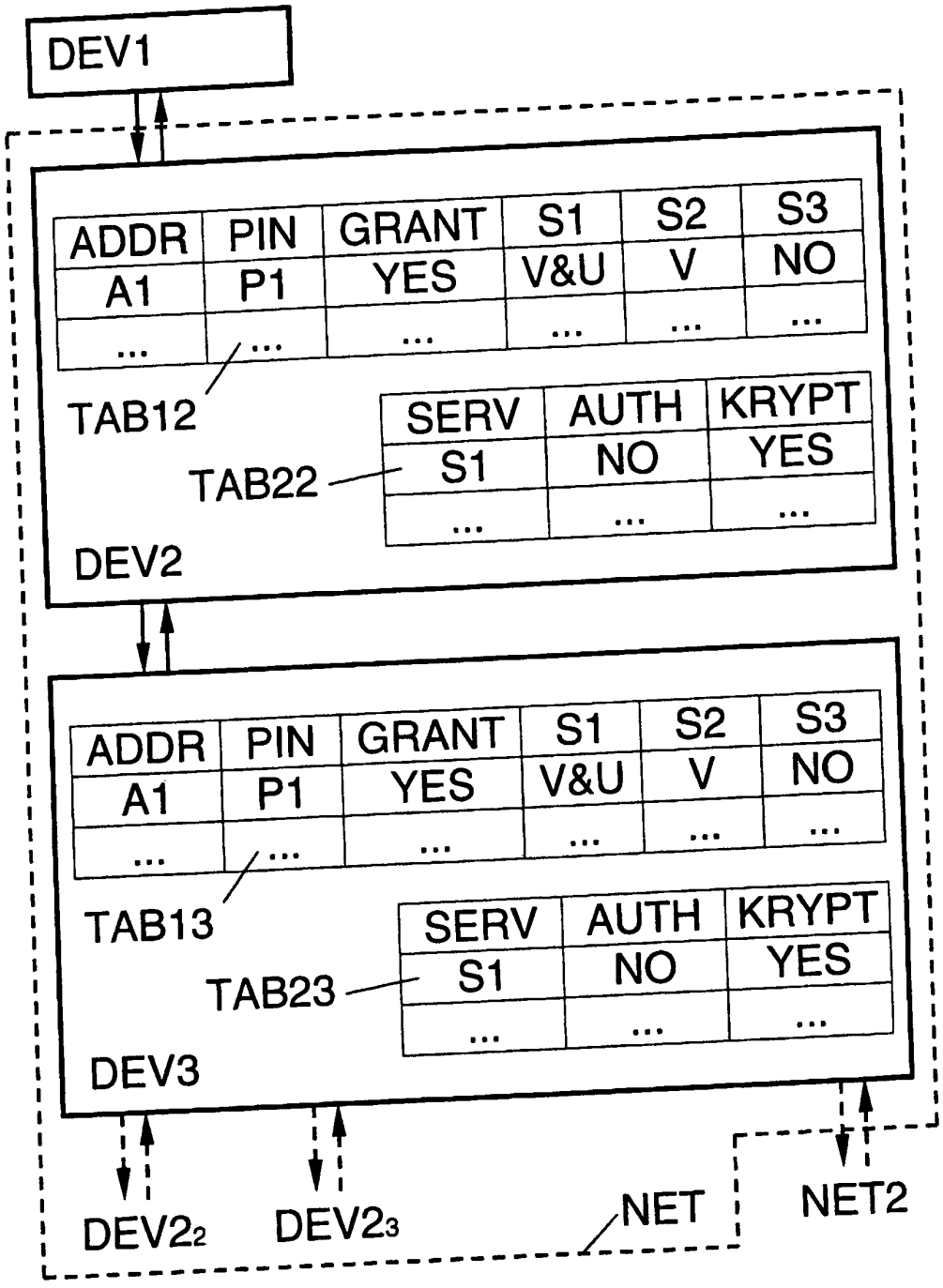

Fig.