(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
17. März 2005 (17.03.2005)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2005/024543 A2

(51) Internationale Patentklassifikation[7]: G06F

(21) Internationales Aktenzeichen: PCT/EP2004/010074

(22) Internationales Anmeldedatum:
6. September 2004 (06.09.2004)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
103 41 873.3 5. September 2003 (05.09.2003) DE

(71) Anmelder und
(72) Erfinder: **BERGS, Magnus H.** [IS/IS]; Morkin 8, IS-108 Reykjavik (IS). **TAVANGARIAN, Djamshid** [DE/DE]; Georg-Büchner-Str. 3, 18055 Rostock (DE).

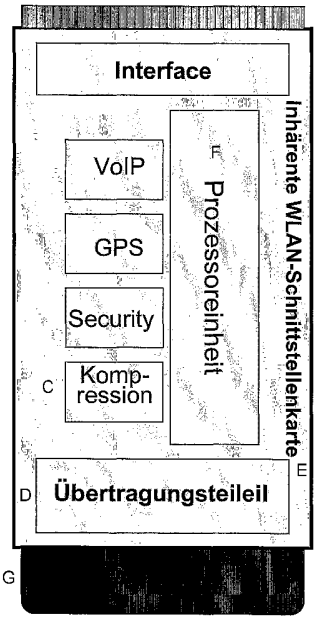
(74) Anwälte: **HENGELHAUPT, Jürgen, D.** usw.; Anwaltskanzlei, Gulde Hengelhaupt Ziebig & Schneider, Wallstr. 58/59, 10179 Berlin (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD AND DEVICE FOR SETTING UP LINKS BETWEEN COMMUNICATION TERMINALS AND DATA AND COMMUNICATION NETWORKS COMPRISING WIRELESS TRANSMISSION PATHS SUCH AS WIRELESS LOCAL AREA NETWORKS (WLAN) AND/OR MOBILE RADIO NETWORKS, AND CORRESPONDING COMPUTER PROGRAM

(54) Bezeichnung: VERFAHREN UND VORRICHTUNG FÜR DEN AUFBAU VON VERBINDUNGEN ZWISCHEN KOMMUNIKATIONSENDGERÄTEN UND DRAHTLOSE ÜBERTRAGUNGSSTRECKEN AUFWEISENDEN DATEN- UND/ODER KOMMUNIKATIONSNETZEN, WIE BEISPIELSWEISE WIRELESS LOCAL AREA NETWORKS (WLAN) UND/ODER MOBILFUNKNETZEN, SOWIE EIN ENTSPRECHENDES COMPUTERPROGRAMM



C... COMPRESSION
D... TRANSMISSION PART
E... INHERENT WLAN INTERFACE CARD
F... PROCESSOR UNIT
G... ANTENNA

(57) **Abstract:** The invention relates to a method and device for setting up links between communication terminals and data and communication networks such as Wireless Local Area Networks (WLAN) and/or mobile radio networks comprising wireless transmission paths, in addition to a corresponding computer program and corresponding computer-readable storage medium which can, in particular, be used in order to create secure access to WLAN networks. According to the invention, a device is used to set up links between communication terminals and data and/or communication networks such as Wireless Local Area Networks (WLAN) and/or mobile radio networks comprising wireless transmission paths. Said device comprises a unit for setting up links with an integrated authentication and/or identification module. The authentication module is configured in such a way that authentication and/or identification for access to the data and/or communication network is carried out by the authentication and/or identification module independently from the operating system of the communication terminal.

(57) **Zusammenfassung:** Die Erfindung betrifft ein Verfahren und eine Vorrichtung für den Aufbau von Verbindungen zwischen Kommunikationsendgeräten und drahtlose Übertragungsstrecken aufweisenden Daten- und/ oder Kommunikationsnetzen, wie bspw. Wireless Local Area Networks (WLAN) und/oder Mobilfunknetzen, sowie ein entsprechendes Computerprogramm und ein entsprechendes computerlesbares Speichermedium, welche insbesondere einsetzbar sind, um einen sicheren Zugang zu WLAN-Netzen aufzubauen. Hierfür wird vorgeschlagen, für den Aufbau von Verbindungen zwischen Kommunikationsendgeräten und drahtlose Übertragungsstrecken aufweisenden Daten- und/oder Kommunikationsnetzen, wie bspw. Wireless Local Area Networks (WLAN) und/oder Mobilfunknetzen, eine Vorrichtung einzusetzen, wobei die Vorrichtung eine Einheit zum Verbindungsaufbau mit integriertem

[Fortsetzung auf der nächsten Seite]

WO 2005/024543 A2

KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Authentisierungs- und/oder Identifikations-Modul umfaßt, wobei das Authentisierungs- und/oder Identifikations-Modul derart eingerichtet ist, daß die Authentisierung und/oder Identifikation für den Zugang zu dem Daten- und/oder Kommunikationsnetz durch das Authentisierungs- und/oder Identifikations-Modul unabhängig vom Betriebssystem des Kommunikationsendgerätes, durchgeführt wird.

Verfahren und Vorrichtung für den Aufbau von Verbindungen zwischen Kommunikationsendgeräten und drahtlose Übertragungsstrecken aufweisenden Daten- und/oder Kommunikationsnetzen, wie bspw. Wireless Local Area Networks (WLAN) und/oder Mobilfunknetzen, sowie ein entsprechendes Computerprogramm und ein entsprechendes computerlesbares Speichermedium

Die Erfindung betrifft ein Verfahren und eine Vorrichtung für den Aufbau von Verbindungen zwischen Kommunikationsendgeräten und drahtlose Übertragungsstrecken aufweisenden Daten- und/oder Kommunikationsnetzen, wie bspw. Wireless Local Area Networks (WLAN) und/oder Mobilfunknetzen, sowie ein entsprechendes Computerprogramm und ein entsprechendes computerlesbares Speichermedium, welche insbesondere einsetzbar sind, um einen sicheren Zugang zu WLAN-Netzen aufzubauen.

Zum jetzigen Zeitpunkt entsteht eine Vielzahl neuer Hotspots in kleineren und größeren WLAN-Netzen. Diese werden durch unterschiedliche Provider mit jeweils eigenen Zugangs- und Abrechnungsverfahren angeboten. Dabei fehlt es bisher an Lösungen, die einerseits eine sichere Zugangsregelung und Abrechnung erlauben und andererseits für einen Nutzer einfach zu handhaben sind und eine transparente Nutzung der Infrastruktur erlauben. Diese Eigenschaften werden in allgegenwärtigen GSM-Netzen mit der dort verwendeten SIM-Karte erreicht. Für WLAN-Netze fehlt bisher eine solche Möglichkeit.

Gegenwärtig existieren verschiedene Verfahren zur Authentisierung bzw. Identifizierung nach IEEE 802.1X (EAP/TLS, LEAP, PEAP). Diese werden von vielen auf dem Markt befindlichen WLAN Access Points unterstützt, wobei je nach Hersteller verschiedene Varianten angeboten werden. Die Authentisierung des Clients erfolgt in derzeitigen Systemen überwiegend per Software. Diese Funktionalität kann im Betriebssystem enthalten sein oder durch eine zusätzliche Software, z.B. vom Hersteller der WLAN-Hardware, vorgenommen werden.

Der Einsatz eines Authentisierungssystems erfordert eine Abstimmung aller an der Authentisierung beteiligten Komoponenten (RADIUS-Server [RADIUS = *Remote Authentication Dial In User Service*], Access Point, WLAN-Hardware, Betriebssystem, Authentisierungssoftware) aufeinander. Die komplexen Abhängigkeiten unter den Komponenten, speziell innerhalb des Clients, sind ein wesentlicher Grund für die geringe Verbreitung.
Ein wesentlicher Nachteil einer Authentisierung mittels Software ist die relativ leichte Angreifbarkeit dieses Prozesses. Auf dem Client muss ein geheimer Schlüssel oder ein Passwort hinterlegt werden. Durch eine Manipulation des Systems, z.B. durch Trojanische Pferde, ist es prinzipiell relativ einfach möglich, an die geheimen Informationen zu gelangen.

Im Rahmen der Weiterentwicklung der aktuellen WLAN-Technik gibt es eine Reihe von Bestrebungen zur Erhöhung der Sicherheit. Der Fokus liegt dabei auf der Sicherheit der Datenübertragung über die Luftschnittstelle. Als wesentlicher Punkt ist hier die der zukünftige Standard IEEE 802.11i (erwartet für 2004) zu nennen. Mit der Verabschiedung des Standards ist damit zu rechnen, dass er in allen neuen Produkten integriert sein wird und auch in viele existierende Geräte durch Firmware-Upgrades nachgerüstet werden kann.
Im Bereich der Authentisierung existiert der Standard 802.1X. Dieser erfordert eine Unterstützung innerhalb des WLAN Access Points, was bei vielen auf dem Markt befindlichen Produkten verschiedener Hersteller gegeben ist. Im Client wird die Funktionalität bei allen bekannten Anwendungen durch Software realisiert, was die bereits erwähnten Nachteile mit sich bringt. Eine weitere Variante ist die Authentisierung mittels Smartcard. Dabei wird die eigentliche Authentisierung innerhalb einer Smartcard durchgeführt, ohne dass die geheime Information diese verlassen muss. Die Vermittlung zwischen WLAN-Karte und Smartcard erfolgt dabei durch das Betriebssystem. Diese Funktion ist z.B. in Windows XP integriert. Der größte Nachteil dieser Variante ist der zusätzlich benötigte Smartcard-Reader. Insbesondere bei kleinen Mobilgeräten, z.B.

PDAs, ist der Einsatz von Smartcards oft nicht möglich bzw. äußerst unpraktisch.

Des weiteren ist aus der deutschen Offenlegungsschrift DE 100 43 203 A1 eine generische WLAN-Architektur bekannt, welche ein Verfahren und ein System zur Nutzung von mehreren Netzen unterschiedlicher Art, beispielsweise die Nutzung von Datennetzen (WLAN) durch Einwahl über ein zellulares Mobilfunknetz (GSM), beschreibt, wobei eines der Netze logische Funktionen von Komponenten des jeweils anderen Netzes generisch bereitstellt.

Eine Integration eines Abrechnungssystems zwischen zellularen und WLAN-Netzwerken wird in der Internationalen Patentanmeldung WO 03/032618 A1 „Integration of Billing between Cellular and WLAN Networks" vorgestellt. Durch diese Lösung wird die Einwahl in Datennetze (LAN) mit Hilfe von Mobiltelefonen (GSM/GPRS) über zellulare Netzwerke ermöglicht. Im Datennetzwerk wird ein (temporärer) Account eingerichtet, der die Gebühren ermittelt und sie anschließend an das Billingsystem des zellularen Netzwerks sendet. Jedoch ermöglicht es diese Lösung nicht, während der Nutzung der Netze zwischen Einwahlpunkten verschiedener Provider der zellularen Netze zu bewegen.

In der deutschen Offenlegungsschrift DE 101 52 572 A1 „Verfahren und Vorrichtung zum authentisierten Zugriff einer Station auf lokale Datennetze, insbesondere Funk-Datennetze" wird ein Verfahren und eine entsprechende Vorrichtung beschrieben, durch welche eine Authentisierung in dem Funk-Datennetz ermöglicht wird, indem Zugangsinformationen für den Zugang zu dem Funk-Datennetz über ein von dem Funk-Datennetz verschiedenes Telekommunikationsnetz, insbesondere per SMS (= Short Message System) über ein Mobilfunknetz, an einen Nutzer übersendet werden.

In der deutschen Offenlegungsschrift DE 101 37 551 A1 „Vorausbezahlte Nutzung spezieller Dienstangebote" wird ein System vorgeschlagen, wobei Dienste eines in einem Telekommunikationsnetz eingerichteten Server genutzt werden können, nachdem

auf dem Server ein Nutzerkonto und ein Nutzerguthaben eingerichtet wurde. Insbesondere wird ein Pre-paid-Verfahren genutzt.

In der Europäischen Patentanmeldung EP 0 970 411 B1 „Datenkopierschutz" wird ein Verfahren zum Schutz von über ein Netzwerk übertragenen Daten vorgestellt. Dabei werden urheberrechtlich geschützte Teile von HTML-Seiten einer besonderen Behandlung unterzogen, um unberechtigte Verwendungen zu verhindern.

Die Aufgabe der Erfindung besteht somit darin, ein Verfahren und eine Vorrichtung für den Aufbau von Verbindungen zwischen Kommunikationsendgeräten und drahtlose Übertragungsstrecken aufweisenden Daten- und/oder Kommunikationsnetzen, wie bspw. Wireless Local Area Networks (WLAN) und/oder Mobilfunknetzen, sowie ein entsprechendes Computerprogramm und ein entsprechendes computerlesbares Speichermedium bereitzustellen, welche die erwähnten Nachteile beheben und insbesondere eine Beeinflussung des Authentisierungs- und/oder Identifikations-Ablaufs durch Dritte verhindern.

Diese Aufgabe wird erfindungsgemäß durch die Merkmale in den Ansprüchen 1, 14, 15, 27 und 28 gelöst. Zweckmäßige Ausgestaltungen der Erfindung sind in den Unteransprüchen enthalten.

Ein besonderer Vorteil des erfindungsgemäßen Verfahrens für den Aufbau von Verbindungen zwischen Kommunikationsendgeräten und drahtlose Übertragungsstrecken aufweisenden Daten- und/oder Kommunikationsnetzen, wie bspw. Wireless Local Area Networks (WLAN) und/oder Mobilfunknetzen, besteht darin, dass sowohl die Speicherung der für eine Authentisierung und/oder Identifikation erforderlichen Daten als auch der Prozeß der Authentisierung und/oder Identifikation ohne Eingriff des Betriebssystems des Kommunikationsendgerätes erfolgt, da Verbindungen durch eine Einheit zum Verbindungsaufbau mit integriertem Authentisierungs- und/oder Identifikations-Modul hergestellt werden, wobei die Authentisierung und/oder Identi-

fikation für den Zugang zu dem Daten- und/oder Kommunikationsnetz durch das Authentisierungs- und/oder Identifikations-Modul unabhängig vom Betriebssystem des Kommunikationsendgerätes, durchgeführt wird.

Eine Vorrichtung nach der Erfindung ist vorteilhafterweise so eingerichtet, dass die Vorrichtung eine Einheit zum Verbindungsaufbau mit integriertem Authentisierungs- und/oder Identifikations-Modul umfaßt, wobei das Authentisierungs- und/oder Identifikations-Modul derart eingerichtet ist, daß die Authentisierung und/oder Identifikation für den Zugang zu dem Daten- und/oder Kommunikationsnetz durch das Authentisierungs- und/oder Identifikations-Modul unabhängig vom Betriebssystem des Kommunikationsendgerätes, durchgeführt wird.

Eine andere Vorrichtung für den Aufbau von Verbindungen zwischen Kommunikationsendgeräten und drahtlose Übertragungsstrecken aufweisenden Daten- und/oder Kommunikationsnetzen, wie bspw. Wireless Local Area Networks (WLAN) und/oder Mobilfunknetzen, ist dadurch ausgezeichnet, dass die Vorrichtung neben einer Einheit zum Verbindungsaufbau ein VoIP-Modul umfaßt, wobei das VoIP-Modul unabhängig von dem Kommunikationsendgerät nutzbar ist.

Ein erfindungsgemäßes Computerprogramm für den Aufbau von Verbindungen zwischen Kommunikationsendgeräten und drahtlose Übertragungsstrecken aufweisenden Daten- und/oder Kommunikationsnetzen, wie bspw. Wireless Local Area Networks (WLAN) und/oder Mobilfunknetzen, ermöglicht es einem Computer, nachdem es in den Speicher des Computers geladen worden ist, ein derartiges Verfahren für den Aufbau von Verbindungen durchzuführen, derart, dass Verbindungen durch eine Einheit zum Verbindungsaufbau mit integriertem Authentisierungs- und/oder Identifikations-Modul hergestellt werden, wobei die Authentisierung und/oder Identifikation für den Zugang zu dem Daten- und/oder Kommunikationsnetz durch das Authentisierungs- und/oder Identifikations-Modul unabhängig vom Betriebssystem des Kommunikationsendgerätes, durchgeführt wird. Ein solches Com-

puterprogramm kann beispielweise als Firmware der erfindungsgemäßen Vorrichtung realisiert sein.

Beispielsweise können diese Computerprogramme (gegen Gebühr oder unentgeltlich, frei zugänglich oder passwortgeschützt) downloadbar in einem Daten- oder Kommunikationsnetz bereitgestellt werden. Die so bereitgestellten Computerprogramme können dann durch ein Verfahren nutzbar gemacht werden, bei dem ein Computerprogramm nach Anspruch 27 aus einem elektronischen Datennetz, wie beispielsweise aus dem Internet, auf eine an das Datennetz angeschlossene Datenverarbeitungseinrichtung heruntergeladen wird.

Für bestimmte Anwendungen kann es sich als vorteilhaft erweisen, wenn ein computerlesbares Speichermedium eingesetzt wird, auf dem ein Programm gespeichert ist, das es einem Computer ermöglicht, nachdem es in den Speicher des Computers geladen worden ist, ein Verfahren für den Aufbau von Verbindungen zwischen Kommunikationsendgeräten und drahtlose Übertragungsstrecken aufweisenden Daten- und/oder Kommunikationsnetzen, wie bspw. Wireless Local Area Networks (WLAN) und/oder Mobilfunknetzen, durchzuführen, derart, dass Verbindungen durch eine Einheit zum Verbindungsaufbau mit integriertem Authentisierungs- und/oder Identifikations-Modul hergestellt werden, wobei die Authentisierung und/oder Identifikation für den Zugang zu dem Daten- und/oder Kommunikationsnetz durch das Authentisierungs- und/oder Identifikations-Modul unabhängig vom Betriebssystem des Kommunikationsendgerätes, durchgeführt wird. Ein solches Computerprogramm kann beispielweise als Firmware der erfindungsgemäßen Vorrichtung realisiert sein.

In einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens ist vorgesehen, daß für den Verbindungsaufbau eine

WLAN-Schnittstellenkarte mit Smartcard-Funktionalität verwendet wird.

In einer anderen bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens ist vorgesehen, daß geheime Informationen wie bspw. private Schlüssel den Sicherheits-Speicherbereich des Authentisierungs- und/oder Identifikations-Moduls nicht verlassen. Damit wird zum Beispiel das Ausspähen von vertraulichen Daten, wie bspw. eines privaten Schlüssels, erschwert. Eine zusätzliche Erhöhung der Sicherheit wird erreicht, wenn bei unbefugtem Zugriff auf das Authentisierungs- und/oder Identifikations-Modul die geheimen Informationen unbrauchbar gemacht werden.

Des weiteren erweist es sich als Vorteil, wenn wenigstens ein Teil der EAPOL-Pakete aus den empfangenen Daten herausgefiltert und durch das Authentisierungs- und/oder Identifikations-Modul ausgewertet wird.

In einer weiteren bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens ist vorgesehen, daß eine Authentisierung nach IEEE 802.1X mit EAP/TLS genutzt wird und/oder kryptographische Verfahren zum Einsatz kommen, bei welchen Zertifikate übertragen werden.

Neben einem Modul zum Verbindungsaufbau kann die erfindungsgemäße Vorrichtung weitere nützliche Funktionalitäten bereitstellen. So ist es beispielsweise von Vorteil, wenn die Einheit zum Verbindungsaufbau ein Modul für paketorientierte Sprachdienste, wie beispielsweise Telefonie über Voice over IP (VoIP) umfaßt, wobei das Modul für paketorientierte Sprachdienste unabhängig vom Betriebssystem des Kommunikationsendgerätes arbeitet.

Für die eigenständige Nutzung von auf der erfindungsgemäßen Vorrichtung implementierten Module erweist es sich als vorteilhaft, wenn die Vorrichtung derart eingerichtet ist, dass

die Energieversorgung der Vorrichtung durch die Energieversorgungseinrichtung des Kommunikationsendgerätes realisierbar ist.

Das Authentisierungs- und/oder Identifikations-Moduls wird in der Regel die sicherheitsrelevanten Daten selbst in einem Sicherheits-Speicherbereich enthalten. Da ein Nutzer aber oftmals bereits andere Authentisierungs- und/oder Identifikations-Daten besitzt, kann es sich als vorteilhaft erweisen, diese auch zur Authentisierung und/oder Identifikation für den Aufbau von Verbindungen zwischen Kommunikationsendgeräten und drahtlose Übertragungsstrecken aufweisenden Daten- und/oder Kommunikationsnetzen, wie bspw. Wireless Local Area Networks (WLAN) und/oder Mobilfunknetzen, zu verwenden. Hierzu ist vorgesehen, dass für die Authentisierung und/oder Identifikation durch das Authentisierungs- und/oder Identifikations-Modul Daten mit einer SIM-Card ausgetauscht werden, und die Authentisierung mit auf der SIM-Card enthaltenen Daten erfolgt. Die SIM-Card ist dabei als Teil des Authentisierungs- und/oder Identifikations-Moduls anzusehen. Insbesondere erweist es sich als vorteilhaft, eine intelligente SIM-Card oder auch eine Smartcard mit zusätzlichen Informationen auf einem geschützten Speicherbereich einzusetzen. Im folgenden sollen Ausführungsformen am Beispiel einer (intelligenten) SIM-Card näher erläutert werden, wobei jedoch anstelle der (intelligenten) SIM-Card stets auch eine Smartcard eingesetzt werden kann.

Die (intelligente) SIM-Card des Authentisierungs- und/oder Identifikations-Moduls kann dabei im gleichen Kommunikationsendgerät installiert sein wie die Einheit zum Verbindungsaufbau. In einem speziellen Ausführungsbeispiel ist das (intelligente) SIM-Card direkt auf der Einheit zum Verbindungsaufbau installiert. In einer alternativen Ausführungsform umfaßt das Authentisierungs- und/oder Identifikations-Modul mehrere Komponenten, wobei die (intelligente) SIM-Card auf einer speziellen, selbständigen Komponente untergebracht ist,

die beispielsweise als eine Art Dongle über eine USB-, Bluetooth-, Infrarot- oder andere Schnittstelle mit dem Kommunikationsendgerät verbunden ist. Es gibt aber auch Fälle, wo die inhärente WLAN-Schnittstellenkarte mit einem Teil des Authentisierungs- und/oder Identifikations-Moduls in einem ersten Kommunikationsendgerät und die (intelligente) SIM-Card in einem zweiten, von dem ersten verschiedenen Kommunikationsendgerät installiert ist. Dies ist etwa der Fall, wenn eine in einem Notebook eingesteckte inhärente WLAN-Schnittstellenkarte Daten von einer (intelligenten) SIM-Card eines Mobiltelefons benutzt. In einem solchen Fall ist es zweckmäßig, wenn der Datenaustausch zwischen Authentisierungs- und/oder Identifikations-Modul und SIM-Card über eine Infrarot- oder Bluetooth-Schnittstelle erfolgt, die in den meisten neueren Kommunikationsendgeräten vorhanden sind. Dafür ist vorgesehen, dass die Vorrichtung eine Schnittstelle zum Datenaustausch mit einer SIM-Card aufweist, wobei die Schnittstelle als Infrarot- oder Bluetooth-Schnittstelle ausgebildet ist. Selbstverständlich sind auch andere Schnittstellen bzw. Protokolle für den Datenaustausch einsetzbar.

In einer bevorzugten Ausführungsform der erfindungsgemäßen Vorrichtung ist vorgesehen, dass das Authentisierungs- und/oder Identifikations-Modul als Hardwarelösung oder als Firmwarelösung realisiert ist.

Insbesondere sieht eine spezielle Ausführungsform vor, dass zur Implementierung des Authentisierungs- und/oder Identifikations-Moduls eine FPGA-Komponente dient.

Vorteilhafterweise umfaßt eine Vorrichtung für den Aufbau von Verbindungen zwischen Kommunikationsendgeräten und drahtlose Übertragungsstrecken aufweisenden Daten- und/oder Kommunikationsnetzen, wie bspw. Wireless Local Area Networks (WLAN) und/oder Mobilfunknetzen, neben einem Authentisierungs- und/oder Identifikations-Modul zusätzlich ein Kompressionsmodul, ein GPS-Modul und/oder ein Modul für paketorientierte Sprach-

dienste, wie beispielsweise Telefonie über Voice over IP (VoIP). In diesem Falle ist vorgesehen, dass die Vorrichtung zusammen mit einem Modul für paketorientierte Sprachdienste, wie beispielsweise Telefonie über Voice over IP (VoIP), eine für ein Head Set geeignete Schnittstelle aufweist.

Durch die Integration der erfindungsgemäßen Smartcard-Funktionalität in die WLAN-Karte wird eine sichere Authentisierung ohne großen Aufwand für eine Vielzahl von Geräten erschlossen. Wahlweise kann diese Funktionalität als hardwarebasierte oder als firmwarebasierte Lösung bereitgestellt werden. Die Ähnlichkeit zu einer Smartcard-Authentisierung besteht darin, dass die geheime Information, der private Schlüssel, nicht aus dem Hardwaremodul herausgelangt. Die zu signierenden Daten werden an das Modul übergeben und das Ergebnis wird zurückgeliefert. Der Zugriff auf die Hardware wird durch technische Maßnahmen soweit eingeschränkt, dass der Zugriff auf die geschützten Informationen mit einem vertretbaren Aufwand nicht möglich ist.
Die Realisierung erfolgt beispielsweise durch eine Erweiterung der karteninternen Software (Firmware). Dieses ist ohne Modifikation der eigentlichen Hardware möglich. Es würde völlig ausreichen, bereits vorhandene Firmware zu erweitern. Die Modifikation der Firmware könnte beispielsweise darin bestehen, alle gesendeten EAPOL (EAP over LAN) Pakete aus den empfangenen Daten herauszufiltern, auszuwerten und zu beantworten. In diesem Falle werden dazu entsprechende kryptographische Funktionen implementiert.

Die erfindungsgemäße Lösung lässt sich in allen WLAN-Anwendungen einsetzen, welche eine sichere Authentisierung bzw. Identifizierung erfordern.

Eine Großflächige WLAN-Vernetzung erfordert eine Vielzahl von Zugangspunkten. Diese WLAN-Hotspots werden dabei in der Regel von unterschiedlichen Betreibern bereitgestellt, die darüber hinaus im allgemeinen auch unterschiedliche Zugangsverfahren

durchführen. Für eine kommerzielle Nutzung sind Mechanismen für die Zugangskontrolle, Zugangsbeschränkung und Abrechnung unerlässlich. Diese setzen eine sichere Authentisierung bzw. Identifizierung des Nutzers voraus. Um die Situation dieser Vielzahl von Zugangserfordernissen, die durch die verschiedenen Provider berücksichtigt werden müssen, zu umgehen, wurde eine Systemarchitektur mit einem zentralisierten Support- und Service-Center (zentraler Service-Stelle für Hotspots) vorgeschlagen, das dann die Zugangsberechtigungen der Nutzer mit einem speziell dafür konzipierten und im Hotspot installierten Proxi (RADIUS-Proxi) überprüft, die Abrechnung von Gebühren für die Clients und für die Hotspots übernimmt sowie umfangreiche Support- und Serviceleistungen anbietet.

In Verbindung mit dieser einheitlichen Struktur können das erfindungsgemäße Zugangsverfahren und die erfindungsgemäße WLAN-Schnittstellenkarte vorteilhaft eingesetzt werden. Der einheitliche Zugang wird mit der erfindungsgemäßen WLAN-Schnittstellenkarte vorgenommen, wobei die WLAN-Schnittstelle mit einer Smartcard-Funktionalität zu einer Einheit kombiniert bzw. verschmolzen wird. Damit kann eine zentralisierte Überprüfung durch Einsatz von privaten Geheimschlüsseln vorgenommen werden, um die Berechtigung des Netzzuganges für einen Klienten sicherzustellen. Das Konzept bietet die höchste Sicherheit, Integrität und Transparenz des Systems für die Nutzer bei der Kommunikation und dem Datenaustausch im Internet

Damit entsteht ein System, welches eine vollständige Infrastruktur für großflächige öffentliche WLAN-Netze mit einem horizontalen Handover liefert, angefangen von sicheren Authentisierungsmöglichkeiten und der Bereitstellung individueller, personalisierter Dienste bis hin zur Nutzerverwaltung und Abrechnung.

Eine sichere Authentisierung wird dadurch erreicht, indem die entsprechenden Mechanismen in die WLAN-Zugangshardware integriert werden. Dazu wird beispielsweise die Authentisierung nach IEEE 802.1X mit EAP/TLS genutzt, und es kommen krypto-

graphische Verfahren zum Einsatz, bei welchen Zertifikate übertragen werden. Das eigentliche Geheimnis, der Schlüssel, verlässt die WLAN-Karte nie. Dadurch ist es nicht ohne wieteres möglich, einen fremden Schlüssel abzuhören oder auszuspähen. Somit erfolgen die Prozesse zur Authentisierung ohne Beteiligung des Betriebssystems, was einerseits keinen zusätzlichen Aufwand für den Nutzer bedeutet und andererseits eine große Systemunabhängigkeit gewährleistet.

Nachfolgend wird die Erfindung unter Bezugnahme auf die Figuren der Zeichnungen an einem Ausführungsbeispiel näher erläutert. Es zeigen:

Figur 1: Veranschaulichung der WLAN- Systemarchitektur bei Einsatz eines zentralen zentralisierten Support- und Service-Centers;

Figur 2: Veranschaulichung der bei einer 802.1X Authentisierung ablaufenden Kommunikationsprozesse;

Figur 3: schematische Darstellung einer Inhärenten WLAN-Schnittstellenkarte mit erweiterter Funktionalität;

Figur 4: Veranschaulichung einer durch ein Voice-Gateway erweiterten Systemarchitektur.

Eine großflächige WLAN-Vernetzung erfordert eine Vielzahl von Zugangspunkten, sogenannten WLAN-Hotspots, die im allgemeinen durch unabhängige Provider mit unterschiedlichen Zugangsverfahren angeboten werden. Für eine kommerzielle Nutzung sind Mechanismen für die Zugangskontrolle, Zugangsbeschränkung und Abrechnung unerlässlich. Diese setzen eine sichere Authentisierung bzw. Identifizierung des Nutzers voraus. Auf dieser Basis ist es möglich, eine Vielzahl von Daten (z.B. Verbindungszeit, Transfervolumen) für Abrechnungszwecke zu erfassen. Dazu muss sicher gestellt werden, dass das Identifizierungsverfahren einige wesentliche Eigenschaften erfüllt:

- Sicherheit: Eine Nutzung des Internetzugangs und der angebotenen Dienste soll nur durch einen authentisierten Nutzer möglich sein. Die Verwendung einer falschen Nutzeridentität soll nahezu ausgeschlossen werden. Damit soll die

höchste, heute verfügbare Datensicherheit für einen Nutzer bereitgestellt werden.

- Kompatibilität: Das verwendete Authentisierungs-/Identifizierungsverfahren soll mit einer Vielzahl von bestehenden und zukünftigen Systemen (Hardware und Software) zusammenarbeiten können, ohne dass für jeden Einzelfall aufwendige Anpassungen erforderlich sind.
- Einfachheit: Der Aufwand zur Einrichtung des Netzzugangs und der Identifizierungs-/Authentisierungsmechanismen soll sich auf ein Minimum beschränken. Es sollen dazu auch keine weitreichenden technischen Kenntnisse erforderlich sein.

Der eigentliche Netzwerkzugang erfolgt über eine große Anzahl von Hotspots (siehe Figur 1). Diese bestehen aus einem oder mehreren Access Points (AP) für die WLAN-Verbindung, einem Router für den Internetzugang und wahlweise weiteren Komponenten für lokale Datenerfassung, Dienste usw. Des weiteren liegt den folgenden Ausführungen die oben erwähnte Systemarchitektur mit zentralisiertem Support- und Service-Center (zentraler Service-Stelle für Hotspots) zugrunde, welches die Zugangsberechtigungen der Nutzer mit einem speziell dafür konzipierten und im Hotspot installierten Proxi (RADIUS-Proxi) überprüft, die Abrechnung von Gebühren für die Clients und für die Hotspots übernimmt sowie umfangreiche Support- und Serviceleistungen anbietet. Die Authentisierung wird zentral durch ein im zentralen Support- und Service-Center eingerichteten Authentication Server überprüft.

Die Zugangskontrolle erfolgt durch den Access Point nach dem Standard IEEE 802.1X (siehe Figur 2). Versucht ein neuer Client, eine Verbindung aufzubauen, fordert der AP von diesem eine Identifizierung 1. Der Client sendet seine Identifikation zum AP 2, welche anschließend vom AP zum Authentication Server weitergeleitet wird 3. Der Authentication Server kann mehrere Anfragen an den Client stellen 4 und anhand der Antworten 5 den Netzwerkzugang erlauben oder ablehnen 6. Erst nach Erhalt der Zugangsgenehmigung ermöglicht 7 der Access Point eine

Verbindung des Clients zum Internet. Um Manipulationen bei der Zugangskontrolle entgegenzuwirken, erfolgt die Übertragung der Zugangsinformationen verschlüsselt.

Die Kommunikation zwischen einem Client und einem Access Point erfolgt über das *Extensible Authentication Protocol* (EAP). Der Informationsaustausch mit dem Authentication Server erfolgt über das Internet mittels *Remote Authentication Dial In User Service* (RADIUS). Neben der Zugangskontrolle dient der RADIUS Server auch der Erfassung der Verbindungsdaten. Diese werden vom Access Point ebenfalls mittels RADIUS übertragen.

In dem zentralen Support- und Service-Center werden alle notwendigen Informationen vom RADIUS-Server gesammelt und in einer zentralen Datenbank hinterlegt. Diese dient der Speicherung aller Informationen, welche zum Betrieb des Systems notwendig sind. Das umfasst Zugangsdaten, Abrechnungsinformationen, Managementdaten usw. Die Auswertung und Abrechnung erfolgt durch ein angeschlossenes Billing-System. Durch die gesammelten Informationen (Verbindungszeit, Transfervolumen, genutzte Dienste) ist eine Vielzahl von verschiedenen Abrechnungsmodellen möglich.

Die erfindungsgemäße WLAN-Schnittstellenkarte enthält neben Modulen für die drahtlose Kommunikation nach den Standards 802.11 b, g, a o.ä. eine Reihe von weiteren Merkmalen. In einer speziellen Ausführungsform ist sie als eine Inhärente WLAN-Schnittstellenkarte mit integrierter Sicherheitsfunktionalität, einem VoIP-Modul für Telefonie ins Fest- bzw. Mobilnetz, einem GPS-Modul zur Ortsbestimmung und einem Kompressionsmodul zur Durchführung von Datenkomprimierungen mit Koprimierungsalgorithmen ausgestattet (vgl. Figur 3).

Das ***Security-Modul*** sorgt für eine sichere Datenübertragung sowohl bei der Authentisierung als auch während der laufenden Kommunikation auf der Basis einer Chiffrierung von Daten mit öffentlichen und privaten Schlüsseln. Dieses Modul wird je nach Anforderungen als eine Hardware- oder als eine Firmware-Lösung realisiert. Die Hardware-Lösung wird z. B. durch eine

FPGA-Komponente implementiert. Der FPGA-Baustein wird derart programmiert, damit bei unbefugtem Eingriff seine Funktionalität zerstört, so dass der geheime Schlüssel nicht wieder gefunden werden kann. Eine Software-Lösung kann wiederum als Firmware-Ergänzung in Betracht gezogen werden.

Zur Optimierung der Datenübertragung sind unterschiedliche ***Kompressions- bzw. Verdichtungsalgorithemen*** bekannt geworden. Durch eine Verdichtung von Daten wird die Menge der zu übertragenden Daten und damit die Übertragungszeiten teilweise in hohem Maße reduziert. In dem vorgeschlagenen System kann die beispielhafte WLAN-Smartcard-Schnittstelle mit einem Verdichtungsalgorithmus entweder als eine Zusatz-Hardware oder als Firmware innerhalb des Steuerprozessors ergänzt werden, um die genannten Vorteile zu erzielen. Die Hadware-Lösung zeichnet sich durch die hohe Geschwindigkeit aus, so dass die Latenzzeit gering bleibt. Als Verdichtungsalgorithmen werden verlustfreie Verfahren zur Gewinnung der originären Daten verwendet, während die verlustbehafteten Verfahren für Video- und Audio-Ströme eingesetzt, da sie bei Verlust von Daten in bestimmten Bereichen unempfindlich sind.

Besonders effektiv kann dieser Kompressions-Modul in Verbindung mit dem zentralisierten Support- und Service-Center eingesetzt werden, denn in diesem Falle können weit leistungsstärkere Kompressionsverfahren genutzt werden, als in herkömmlichen Netzen, in denen lediglich einfache Kompressionsverfahren eingesetzt werden können. Der Einsatz von Verfahren mit hoher Komprimierung würde vor allem sie Akzeptanz von vielfältigen Inhalten, wie bspw. Video-on-Demand o.ä., stark erhöhen, da so die Download-Zeiten und somit die Kosten erheblich reduziert würden.

Das ***GPS-Modul*** ist für Lokalisierung des Nutzers verwendet, um dem Nutzer Dienste mit lokalem Kontext zur Verfügung stellen zu können. Hier wird mit dem Modul entweder in gleichmäßig periodischen Zeitpunkten oder je nach Bedarf, z. B. falls eine Anfrage vorliegt, die Lokalisierung des Gerätes vorgenommen und dem zentralen Support-Center mitgeteilt, in dem die notwendigen Informationen bereitgestellt werden. Damit wird die

Aufgaben zu „Local-Based-Support" für optimale Unterstützung des Nutzers bei ortsbezogenen Diensten erreicht.

Das ***VoIP-Modul*** soll, wie der Name darstellt, einen paket-orientierten Sprach-Dienst bereitstellen. Ein Gespräch erfolgt über das mobile Endgerät entlang der Kommunikationsstrecke zwischen dem Endgerät und dem zentralen Support-Center, wo mit Hilfe eines Gateway eine Verbindung zum PSTN oder eines der mobilen Provider hergestellt wird. Auch umgekehrt können die ankommenden Anrufe für den jeweiligen Nutzer auf dem gleichen Weg weitervermittelt werden. Gespräche innerhalb der Hotspots können nach Methoden der VoIP mit bisher bekannt gewordenen Protokollen wie beispielsweise H323 und SIP erfolgen. Durch die vorgesehenen Sicherheitsmechanismen werden auch die Gespräche mit entsprechenden Verschlüsselungen versehen.

In einem speziellen Ausführungsbeispiel ist vorgesehen, dass die VoIP-Verbindung allein über das ***VoIP-Modul*** der Schnittstellenkarte hergestellt und aufrechterhalten wird, ohne den Prozessor und ohne das Betriebssystem des Kommunikationsendgerätes zu nutzen. Die Schnittstellenkarte weist hierfür Anschlußmöglichkeiten für ein Head Set auf. Die VoIP-Funktionalität wird damit allein von der Schnittstellenkarte bereitgestellt, und eine Nutzung dieser VoIP-Funktionalität ist somit von einer Installation entsprechender Applikationen auf dem Kommunikationsendgerät unabhängig.

Eine weitere Anwendungsmöglichkeit eines solchen VoIP-Moduls besteht darin, dieses VoIP-Modul allein mit einer herkömmlichen WLAN-Schnittstellenkarte zu kombinieren. Damit würde ein mobiles WLAN-fähiges VoIP-Telefon bereitgestellt, welches darüber hinaus über eine Schnittstelle für weitere Kommunikationsendgeräte, wie beispielsweise Notebooks oder PDA's, verfügt und so außerdem als Schnittstellenkarte für diese Kommunikationsendgeräte genutzt werden kann, um diesen Kommunikationsendgeräten den Zugang zu einem WLAN-Netz zu ermöglichen.

Um die eigenständige Nutzung von auf der WLAN-Schnittstellenkarte implementierten Funktionalitäten, wie bspw. der VoIP-Funktionalität, zu ermöglichen, wird in einem speziellen Aus-

führungsbeispiel für die Stromversorgung der Schnittstellenkarte die Stromversorgungseinheit des Kommunikationsendgerätes genutzt.

In einer weiteren Ausführungsform werden für die Authentisierung Schnittstellen der Kommunikationsendgeräte genutzt. Die meisten neuen Kommunikationsendgeräte wie Notebooks oder PDA's verfügen über drahtlose Schnittstellen wie etwa Infrarot- oder Funk-Schnittstellen (Bluetooth). Um eine weitere Vereinheitlichung der Nutzerverwaltung zu erreichen, können für die Authentisierung eines Nutzers bei der Einwahl beispielsweise in das Internet oder speziell auch in ein Daten- oder Kommunikationsnetz, welches eine Systemarchitektur mit einem zentralisierten Support- und Service-Center aufweist, auch die Sicherheits- bzw. Identitätsfunktionen genutzt werden, die von einer SIM-Card bereitgestellt werden. Die SIM-Card müßte sich nicht in dem Kommunikationsendgerät befinden, sondern könnte sich in einem weiteren, über eine entsprechende Schnittstelle kontaktierbaren Gerät, beispielsweise einem bluetooth-fähigen Mobiltelefon, befinden. Um die Funktionen der SIM-Card zu nutzen, baut das in der Einheit zum Verbindungsaufbau integrierte Sicherheitsmodul eine Verbindung zu der SIM-Card auf und tauscht die erforderlichen Informationen mit der SIM-Card und dem Authentication Server im Kommunikationsnetz aus. Das integrierte Sicherheitsmodul operiert dabei sozusagen als Mittler. Es sei jedoch betont, dass die Authentisierung selbst durch das Sicherheitsmodul erfolgt und nicht separat durch die SIM-Card. Die SIM-Card kommuniziert bei diesem Verfahren nicht mit dem Netz und speziell nicht mit dem GPRS- oder GSM-System, sondern die Authentisierung erfolgt ausschließlich über den Internetprovider, mit dem der Nutzer eine Netzzugangs-Vereinbarung geschlossen hat, speziell beispielsweise über den Authentication Server des zentralisierten Support- und Service-Centers.

Analog kann die erforderliche Verbindung zwischen der erfindungsgemäßen Vorrichtung zum Verbindungsaufbau und der SIM-

Card auch auf andere Art hergestellt werden, z.B. durch eine elektrische Verbindung der SIM-Card mit einem Steckplatz für die WLAN-Schnittstellenkarte. Diese Ausführungsvariante ist z.B. vorgesehen, wenn sich in dem Kommunikationsendgerät selbst eine SIM-Card befindet, wie das zum Beispiel in sogenannten Smart Phones - internet- und multimediafähigen Mobiltelefonen - der Fall ist.

Die Erfindung beschränkt sich in ihrer Ausführungsform nicht auf die vorstehend angegebenen bevorzugten Ausführungsbeispiele. Vielmehr ist eine Anzahl von Varianten denkbar, die von dem erfindungsgemäßen System und dem erfindungsgemäßen Verfahren auch bei grundsätzlich anders gearteten Ausführungen Gebrauch machen.

Patentansprüche

1. Verfahren für den Aufbau von Verbindungen zwischen Kommunikationsendgeräten und drahtlose Übertragungsstrecken aufweisenden Daten- und/oder Kommunikationsnetzen, wie bspw. Wireless Local Area Networks (WLAN) und/oder Mobilfunknetzen,

   dadurch gekennzeichnet, daß

   Verbindungen durch eine Einheit zum Verbindungsaufbau mit integriertem Authentisierungs- und/oder Identifikations-Modul hergestellt werden, wobei die Authentisierung und/oder Identifikation für den Zugang zu dem Daten- und/oder Kommunikationsnetz durch das Authentisierungs- und/oder Identifikations-Modul unabhängig vom Betriebssystem des Kommunikationsendgerätes, durchgeführt wird.

2. Verfahren nach Anspruch 1,

   dadurch gekennzeichnet, daß

   für den Verbindungsaufbau eine WLAN-Schnittstellenkarte mit inhärenter Smartcard-Funktionalität verwendet wird.

3. Verfahren nach einem der Ansprüche 1 oder 2,

   dadurch gekennzeichnet, daß

   geheime Informationen wie bspw. private Schlüssel den Sicherheits-Speicherbereich des Authentisierungs- und/oder Identifikations-Moduls nicht verlassen.

4. Verfahren nach einem der voranstehenden Ansprüche,

   dadurch gekennzeichnet, daß

   wenigstens ein Teil der EAPOL-Pakete aus den empfangenen Daten herausgefiltert und durch das Authentisierungs- und/oder Identifikations-Modul ausgewertet wird.

5. Verfahren nach einem der voranstehenden Ansprüche,

dadurch gekennzeichnet, daß

eine Authentisierung nach IEEE 802.1X mit EAP/TLS genutzt wird und/oder kryptographische Verfahren zum Einsatz kommen, bei welchen Zertifikate übertragen werden.

6. Verfahren nach einem der voranstehenden Ansprüche,

dadurch gekennzeichnet, daß

bei unbefugtem Zugriff auf das Authentisierungs- und/oder Identifikations-Modul die geheimen Informationen unbrauchbar gemacht werden.

7. Verfahren nach einem der voranstehenden Ansprüche,

dadurch gekennzeichnet, daß

die Einheit zum Verbindungsaufbau ein Modul für paketorientierte Sprachdienste, wie beispielsweise Telefonie über Voice over IP (VoIP) umfaßt, wobei das Modul für paketorientierte Sprachdienste unabhängig vom Betriebssystem des Kommunikationsendgerätes arbeitet.

8. Verfahren nach einem der voranstehenden Ansprüche,

dadurch gekennzeichnet, daß

für die Authentisierung und/oder Identifikation durch das Authentisierungs- und/oder Identifikations-Modul Daten mit einer SIM-Card oder einer Smartcard ausgetauscht werden, und die Authentisierung mit auf der SIM-Card oder auf der Smartcard enthaltenen Daten erfolgt.

9. Verfahren nach einem der voranstehenden Ansprüche,

dadurch gekennzeichnet, daß

ein mehrere Komponenten umfassendes Authentisierungs- und/oder Identifikations-Modul verwendet wird.

10. Verfahren nach einem der Ansprüche 8 oder 9,

dadurch gekennzeichnet, daß

die Einheit zum Verbindungsaufbau und SIM-Card oder die Einheit zum Verbindungsaufbau und Smartcard im gleichen Kommunikationsendgerät installiert sind.

11. Verfahren nach einem der Ansprüche 8 oder 9,

dadurch gekennzeichnet, daß

die die SIM-Card oder die Smartcard enthaltende Komponente als Dongle mit dem Kommunikationsendgerät verbunden ist.

12. Verfahren nach einem der Ansprüche 8 oder 9,

dadurch gekennzeichnet, daß

eine erste Komponente des Authentisierungs- und/oder Identifikations-Moduls zusammen mit der Einheit zum Verbindungsaufbau in einem ersten Kommunikationsendgerät und eine zweite, die SIM-Card oder die Smartcard enthaltende, Komponente des Authentisierungs- und/oder Identifikations-Moduls in einem zweiten, von dem ersten verschiedenen Kommunikationsendgerät installiert sind.

13. Verfahren nach Anspruch 12,

dadurch gekennzeichnet, daß

der Datenaustausch zwischen der ersten Komponente des Authentisierungs- und/oder Identifikations-Moduls und der zweiten, die SIM-Card enthaltenden, Komponente des Authentisierungs- und/oder Identifikations-Moduls über eine Infrarot- oder Bluetooth-Schnittstelle erfolgt.

14. Vorrichtung für den Aufbau von Verbindungen zwischen Kommunikationsendgeräten und drahtlose Übertragungsstrecken aufweisenden Daten- und/oder Kommunikationsnetzen, wie bspw. Wireless Local Area Networks (WLAN) und/oder Mobilfunknetzen,

dadurch gekennzeichnet, daß

die Vorrichtung eine Einheit zum Verbindungsaufbau mit integriertem Authentisierungs- und/oder Identifikations-Modul umfaßt, wobei das Authentisierungs- und/oder Identifikations-Modul derart eingerichtet ist, daß die Authentisierung und/oder Identifikation für den Zugang zu dem Daten- und/oder Kommunikationsnetz durch das Authentisierungs- und/oder Identifikations-Modul unabhängig vom Betriebssystem des Kommunikationsendgerätes, durchgeführt wird.

15. Vorrichtung für den Aufbau von Verbindungen zwischen Kommunikationsendgeräten und drahtlose Übertragungsstrecken aufweisenden Daten- und/oder Kommunikationsnetzen, wie bspw. Wireless Local Area Networks (WLAN) und/oder Mobilfunknetzen,

dadurch gekennzeichnet, daß

die Vorrichtung neben einer Einheit zum Verbindungsaufbau ein VoIP-Modul umfaßt, wobei das VoIP-Modul unabhängig von dem Kommunikationsendgerät nutzbar ist.

16. Vorrichtung nach Anspruch 14,

dadurch gekennzeichnet, daß

die Vorrichtung als WLAN-Schnittstellenkarte mit inhärenter Smartcard-Funktionalität ausgebildet ist.

17. Vorrichtung nach Anspruch 14 oder 16,

dadurch gekennzeichnet, daß

das Authentisierungs- und/oder Identifikations-Modul als Hardwarelösung oder als Firmwarelösung realisiert ist.

18. Vorrichtung nach Anspruch 14,

dadurch gekennzeichnet, daß

zur Implementierung des Authentisierungs- und/oder Identifikations-Moduls eine FPGA-Komponente dient.

19. Vorrichtung nach einem der Ansprüche 14 bis 18,

dadurch gekennzeichnet, daß

die Vorrichtung
- ein Kompressionsmodul,
- ein GPS-Modul und/oder
- ein Modul für paketorientierte Sprachdienste, wie beispielsweise Telefonie über Voice over IP (VoIP),

umfaßt.

20. Vorrichtung nach einem der Ansprüche 14 bis 19,

dadurch gekennzeichnet, daß

das Authentisierungs- und/oder Identifikations-Modul mehrere Komponenten umfaßt.

21. Vorrichtung nach Anspruch 20,

dadurch gekennzeichnet, daß

eine Komponente des Authentisierungs- und/oder Identifikations-Moduls als Dongle ausgebildet ist.

22. Vorrichtung nach einem der Ansprüche 20 oder 21,

dadurch gekennzeichnet, daß

eine Komponente des Authentisierungs- und/oder Identifikations-Moduls eine SIM-Card oder eine Smartcard umfaßt.

23. Vorrichtung nach einem der Ansprüche 14 bis 22,

dadurch gekennzeichnet, daß

die Vorrichtung eine Schnittstelle zum Datenaustausch mit einer SIM-Card oder Smartcard aufweist.

24. Vorrichtung nach Anspruch 23,

dadurch gekennzeichnet, daß

die Schnittstelle als Infrarot-, USB- oder Bluetooth-Schnittstelle ausgebildet ist.

25. Vorrichtung nach Anspruch 15,

dadurch gekennzeichnet, daß

die Vorrichtung zusammen mit einem Modul für paket-orientierte Sprachdienste, wie beispielsweise Telefonie über Voice over IP (VoIP), eine für ein Head Set geeignete Schnittstelle aufweist.

26. Vorrichtung nach einem der Ansprüche 14 bis 25,

dadurch gekennzeichnet, daß

die Vorrichtung derart eingerichtet ist, dass die Energieversorgung der Vorrichtung durch die Energieversorgungseinrichtung des Kommunikationsendgerätes realisierbar ist.

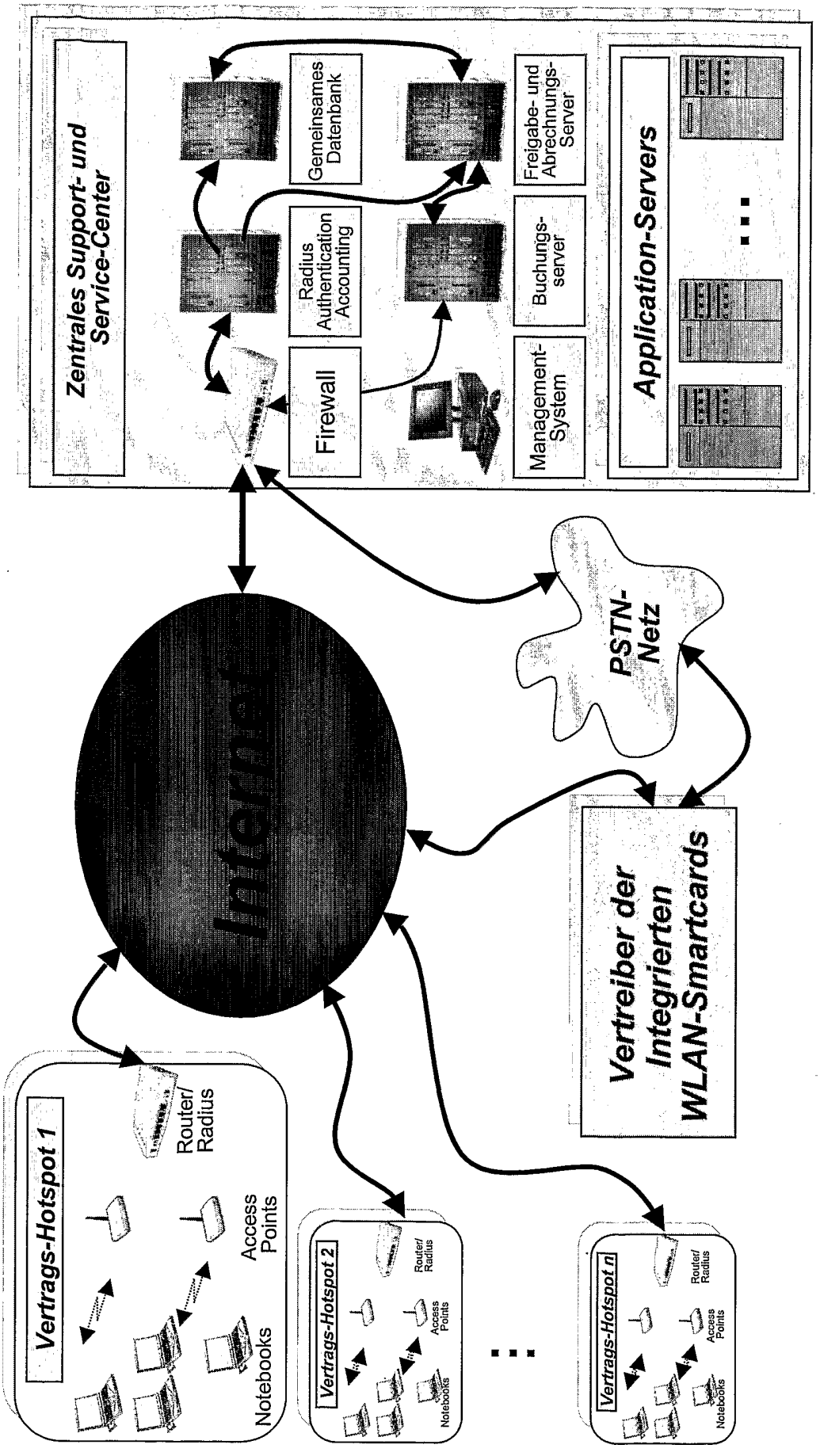
27. Computerprogramm, das es einem Computer ermöglicht, nachdem es in den Speicher des Computers geladen worden ist, ein Verfahren für den Aufbau von Verbindungen zwischen Kommunikationsendgeräten und drahtlose Übertragungsstrecken aufweisenden Daten- und/oder Kommunikationsnetzen, wie bspw. Wireless Local Area Networks (WLAN) und/oder Mobilfunknetzen, durchzuführen, derart, dass Verbindungen durch eine Einheit zum Verbindungsaufbau mit integriertem Authentisierungs- und/oder Identifikations-Modul hergestellt werden, wobei die Authentisierung und/oder Identifikation für den Zugang zu dem Daten- und/oder Kommunikationsnetz durch das Authentisierungs- und/oder Identifikations-Modul unabhängig vom Betriebssystem des Kommunikationsendgerätes, durchgeführt wird.

28. Computerlesbares Speichermedium, auf dem ein Programm gespeichert ist, das es einem Computer ermöglicht, nachdem es in den Speicher des Computers geladen worden ist, ein

Verfahren für den Aufbau von Verbindungen zwischen Kommunikationsendgeräten und drahtlose Übertragungsstrecken aufweisenden Daten- und/oder Kommunikationsnetzen, wie bspw. Wireless Local Area Networks (WLAN) und/oder Mobilfunknetzen, durchzuführen, derart, dass Verbindungen durch eine Einheit zum Verbindungsaufbau mit integriertem Authentisierungs- und/oder Identifikations-Modul hergestellt werden, wobei die Authentisierung und/oder Identifikation für den Zugang zu dem Daten- und/oder Kommunikationsnetz durch das Authentisierungs- und/oder Identifikations-Modul unabhängig vom Betriebssystem des Kommunikationsendgerätes, durchgeführt wird.

29. Verfahren, bei dem ein Computerprogramm nach Anspruch 27 aus einem elektronischen Datennetz, wie beispielsweise aus dem Internet, auf eine an das Datennetz angeschlossene Datenverarbeitungseinrichtung heruntergeladen wird.

Fig. 1


Zentrales Support- und Service-Center
Gemeinsames Datenbank
Radius Authentication Accounting
Buchungs-server
Freigabe- und Abrechnungs-Server
Firewall
Management-System
Application-Servers
Internet
PSTN-Netz
Vertreiber der Integrierten WLAN-Smartcards
Vertrags-Hotspot 1
Router/ Radius
Access Points
Notebooks
Vertrags-Hotspot 2
Router/ Radius
Access Points
Notebooks
Vertrags-Hotspot n
Router/ Radius
Access Points
Notebooks

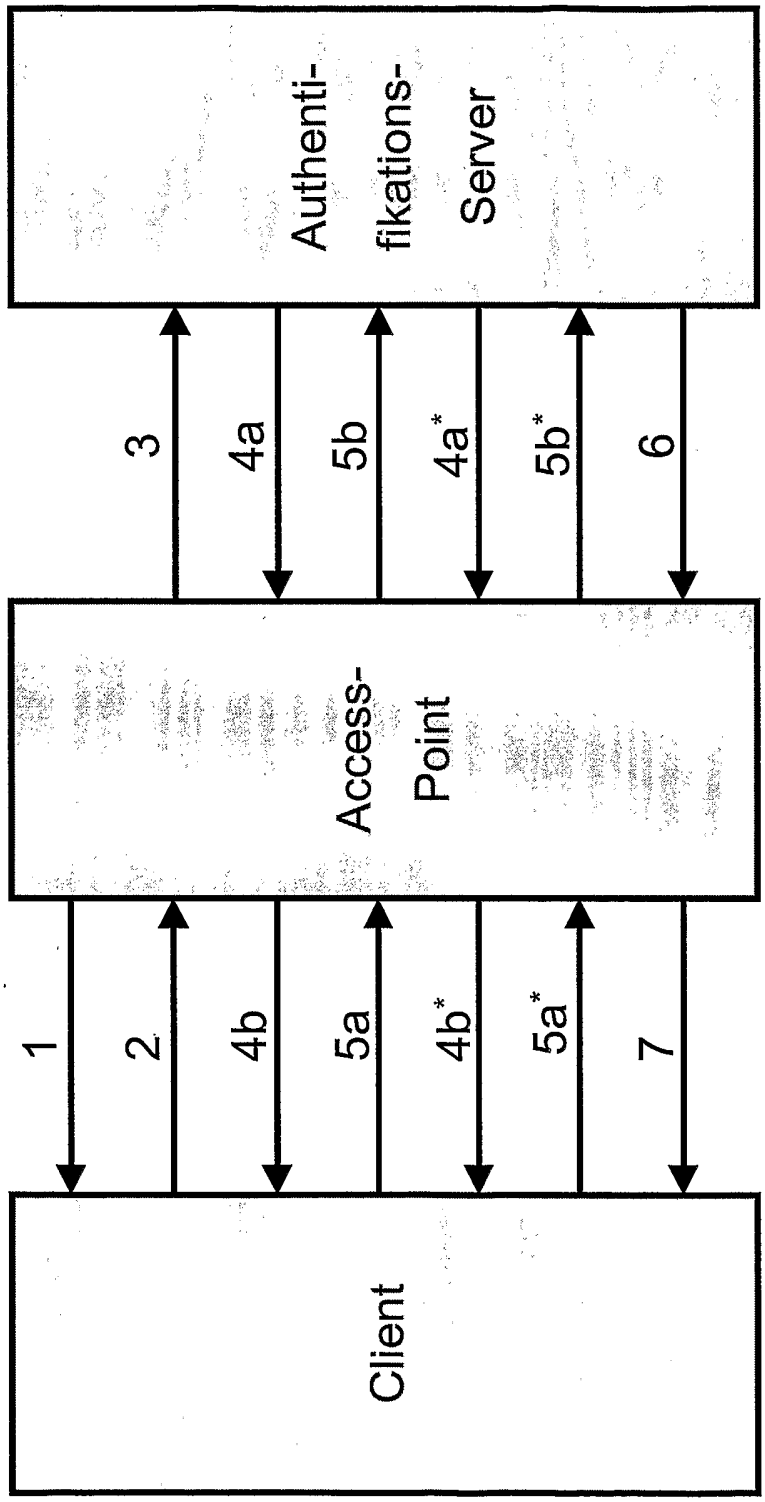

Authenti-
fikations-
Server
Access-
Point
Client
1
2
3
4a
4b
5a
5b
4a*
4b*
5a*
5b*
6
7

Fig. 2

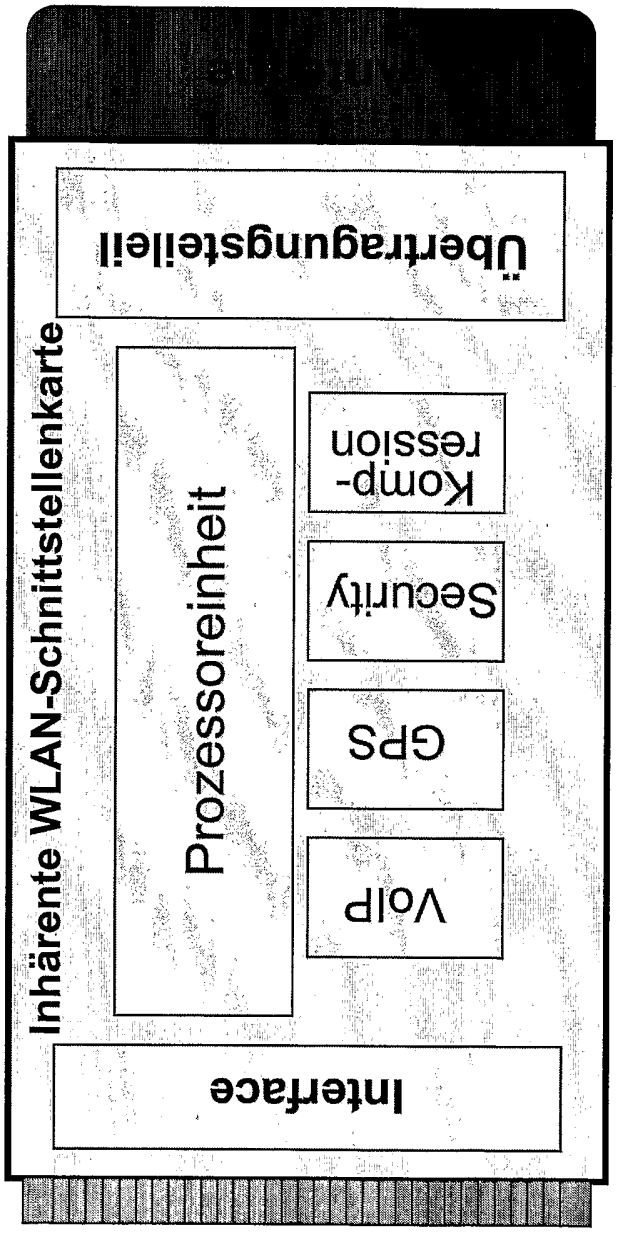
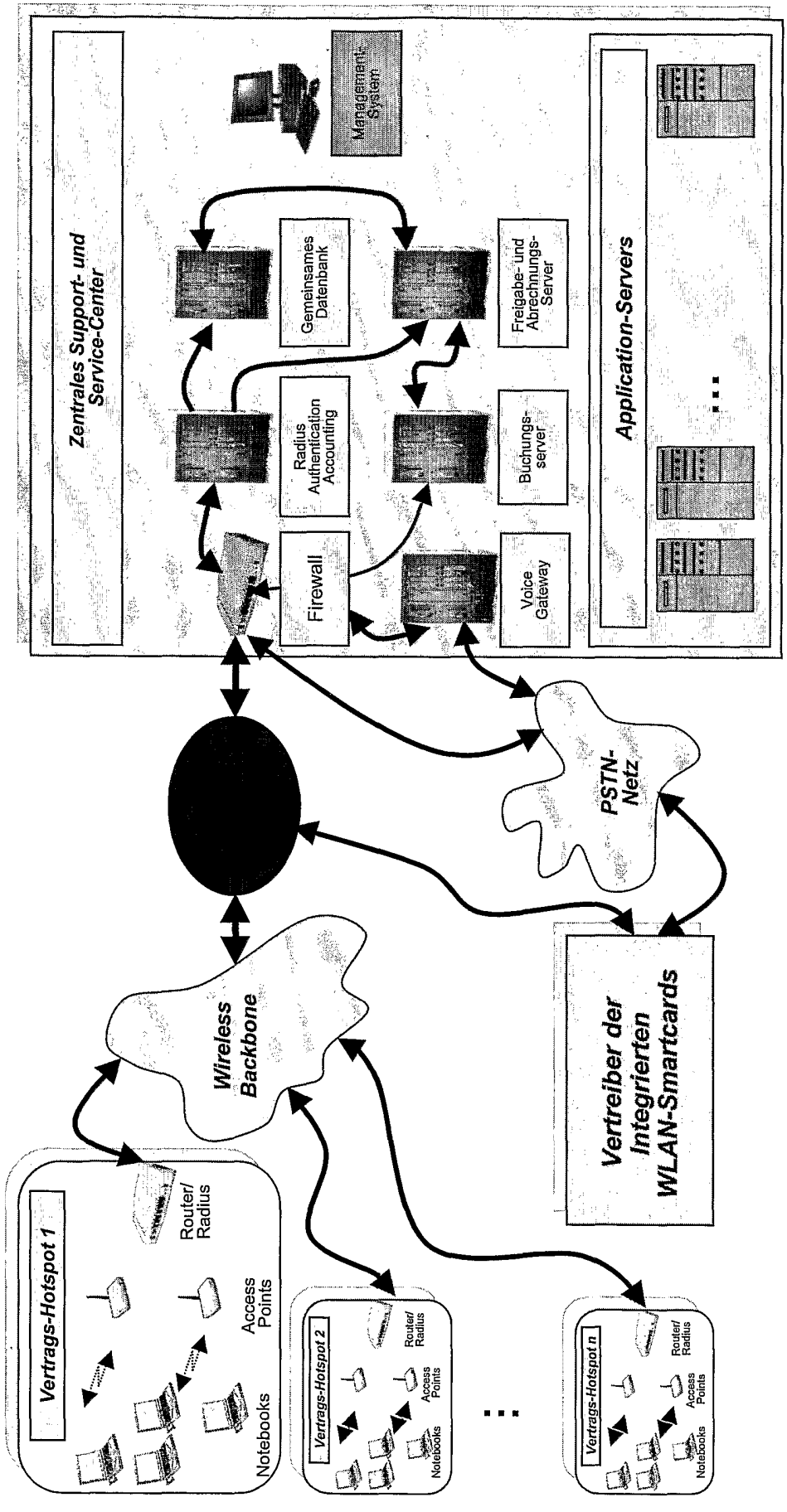

Übertragungsteileil
Inhärente WLAN-Schnittstellenkarte
Prozessoreinheit
Komp-ression
Security
GPS
VoIP
Interface

Fig. 3

Fig. 4


Zentrales Support- und Service-Center
Management-System
Gemeinsames Datenbank
Radius Authentication Accounting
Firewall
Freigabe- und Abrechnungs-Server
Buchungs-server
Voice Gateway
Application-Servers
PSTN-Netz
Wireless Backbone
Vertreiber der Integrierten WLAN-Smartcards
Vertrags-Hotspot 1
Router/ Radius
Access Points
Notebooks
Vertrags-Hotspot 2
Router/ Radius
Access Points
Notebooks
Vertrags-Hotspot n
Router/ Radius
Access Points
Notebooks