(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 602 23 951 T2** 2008.11.27

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 502 388 B1**
(21) Deutsches Aktenzeichen: **602 23 951.6**
(86) PCT-Aktenzeichen: **PCT/EP02/04865**
(96) Europäisches Aktenzeichen: **02 724 305.4**
(87) PCT-Veröffentlichungs-Nr.: **WO 2003/094438**
(86) PCT-Anmeldetag: **01.05.2002**
(87) Veröffentlichungstag der PCT-Anmeldung: **13.11.2003**
(97) Erstveröffentlichung durch das EPA: **02.02.2005**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **05.12.2007**
(47) Veröffentlichungstag im Patentblatt: **27.11.2008**

(51) Int Cl.[8]: ***H04L 12/28*** (2006.01)

(73) Patentinhaber:
Telefonaktiebolaget LM Ericsson (publ), Stockholm, SE

(74) Vertreter:
HOFFMANN & EITLE, 81925 München

(84) Benannte Vertragsstaaten:
AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LI, LU, MC, NL, PT, SE, TR

(72) Erfinder:
GREGORIO RODRIGUEZ, Jesús Angel de, 28660 Boadilla del Monte (Madrid), ES; MONJAS LLORENTE, Miguel Angel, 28045 Madrid, ES

(54) Bezeichnung: **System, Apparat und Methode zur SIM basierten Authentifizierung und Verschlüsselung beim Zugriff auf ein drahtloses lokales Netz**

Beschreibung

Technisches Gebiet der Erfindung

[0001] Die vorliegende Erfindung bezieht sich allgemein auf Authentifizierungs- und Verschlüsselungsmechanismen in Szenarien von drahtlosen Lokalnetzwerken. Insbesondere bezieht sich die Erfindung auf ein Mittel, ein System und Verfahren für eine SIM-basierte Authentifizierung und einen Schicht-2 bzw. Lager-2 Verschlüsselungsmechanismus zum Schützen des Kommunikationspfads ab der Endgerätapparatur nach vorn.

Hintergrund

[0002] Im Jahre 1999 wurde von der IEEE die Spezifikation 802.11b für drahtlosen Lokalnetz(WLAN)zugang mit Raten von 11 Mbps veröffentlicht. Dieser Standard wurde von der Industrie breit unterstützt und weist eine enorme installierte Basis in wirtschaftlichen Unternehmen und ebenso in öffentlich zugänglichen Hot Spots, wie etwa in Flughäfen, Hotels, Cafes usw. auf.

[0003] Diese Spezifikation 802.11b bietet zu einem gewissen Grad Authentifizierungs- und Zugangssteuerungsmechanismen ebenso wie Vertraulichkeit, jedoch nur in dem drahtlosen Pfad. In dieser Hinsicht werden in diesem Standard zwei Authentifizierungsverfahren definiert, nämlich "offenes System" (Englisch: „Open System") und „gemeinsamer Schlüssel" (Englisch: „Shared Key").

[0004] Wenn das offene System benutzt wird, kündigt eine WLAN Karte in der Endgerätvorrichtung (TE, Englisch: Terminal Equipment) an, dass sie wünscht, sich mit einem WLAN Zugangspunkt (im Folgenden als AP, Englisch: Access Point abgekürzt) zu assoziieren. Es wird keine Authentifizierung ausgeführt und es werden nur einige grundlegende Zugangssteuerungsmechanismen benutzt, wie z. B. etwa Medienzugangssteuerungs (MAC, Englisch: Media Access Control)-Filter und Dienstsatzbezeichner (SSID, Englisch: Service Set Identifier).

[0005] Diese MAC Filter sind dazu ausgebildet, dass sie so funktionieren, dass es nur solchen WLAN Karten erlaubt wird, sich mit dem AP zu assoziieren, deren MAC Adresse zu einer in dem AP gehaltenen Liste, wie etwa einer Zugangssteuerungsliste (ACL, Englisch: Access Control List), gehört. Dieser Zugangssteuerungsmechanismus weist eine begrenzte Zweckmäßigkeit auf, weil die Identität der Einheit, die versucht, sich zu assoziieren, nicht tatsächlich zu einem Benutzer gehört, sondern stattdessen zu dem Gerät selbst. Wenn ein Endgerät oder eine Karte gestohlen wird, dann gibt es keine benutzerbasierte Authentifizierung, um einen Zugang mittels der gestohlenen Geräte zu den Ressourcen zu verhindern. Des Weiteren ist das Verschleiern von MAC Adressen ein trivialer Angriff, weil die MAC Adressen der WLAN Karte immer in den Nachrichtenköpfen der WLAN Datenrahmen erscheinen. Dies ist von einer besonderen Relevanz, weil die meisten WLAN Karten auf dem Markt ihre MAC Adresse verändern können, indem sie nur Softwaremittel benutzen.

[0006] Der andere Zugangssteuerungsmechanismus ist der vorgenannte Dienstsatzbezeichner (SSID). Dies ist ein alphanumerischer Code, der den Umstand desjenigen WLAN, mit dem sich die Endgerätvorrichtung (TE) zu assoziieren versucht, identifiziert. Ein gegebener AP erlaubt nur die Assoziierung mit WLAN Karten, die einen richtigen SSID bereitstellen. Jedoch gilt, dass weil dieser Bezeichner normalerweise durch die AP's als Sammelruf ausgesendet wird, und selbst ohne den vom Verkäufer bzw. Anbieter eingestellten Voreinstellungswert zu verändern, ist dieser Zugangssteuerungsmechanismus wiederum ziemlich nutzlos, weil eine Vielzahl wohlbekannter Angriffe auftreten kann.

[0007] Ein zweites oben genanntes Authentifizierungsverfahren ist der sogenannte „gemeinsame Schlüssel" (Englisch: Shared Key). Dieses Verfahren ist in einen grundlegenden Vertraulichkeitsmechanismus eingebettet, welcher von dem verdrahteten äquivalenten Geheimhaltungs (WEP, Englisch: Wired Equivalent Privacy)-Standard bereitgestellt wird. Der WEP-Standard ist ein auf RC4 basierter, symmetrischer Verschlüsselungsalgorithmus. Die Authentifizierung als solche wird ausgeführt, indem ein Anforderungs-Antwortmechanismus benutzt wird, bei dem beide Parteien, die WLAN Karte und der AP zeigen, dass sie einen gleichen Schlüssel besitzen. Jedoch ist dieser Schlüssel in der Endgerätvorrichtung (TE) installiert und gespeichert, und folglich leidet dieser unter denselben Nachteilen wie die beim Besprechen der MAC Filter beschriebenen.

[0008] Darüber hinaus hat eine Anzahl von kürzlich veröffentlichenden Artikeln die fundamentellen Mängel des Geheimhaltungsmechanismus selbst gezeigt, d. h. die Mängel des WEP Standards. Diese Mängel beginnen bei der Benutzung von statischen WEP Schlüsseln, die es einem Angreifer ermöglichen, die Schlüssel selbst zu finden, weil die Initialisierungsvektoren des Algorithmus in der Klarheit innerhalb des WEP Datenrahmens gesendet werden. Eine Anzahl von passiven Angriffen, wie z. B. etwa eine WLAN Karte, die nur den Datenverkehr erschnüffelt, ermöglicht ebenfalls, die Schlüssel abzuleiten.

[0009] Im Anfang erschien es, dass nur durch Erneuern (Englisch: Refreshing) der Schlüssel mit einem besseren Schlüsselmanagement und durch Vergrößern ihrer Länge auf beispielsweise 40 bis 128 Bits der Algorithmus sicherer werden könnte, oder

zumindest sicher genug, um eine akzeptable Sicherheit zu erzielen,. Jedoch haben mehr und mehr kürzliche Berichte bewiesen, dass der Entwurf dieses Algorithmus als solcher keinen akzeptablen Sicherheitsgrad bereitstellen kann.

[0010] Heutzutage werden Anstrengungen von der Industrie und repräsentativen Foren unternommen, um die Mängel in den derzeit verfügbaren Standards zu beheben. Die IEEE ist dabei, einen neuen Standard zu definieren, um den Authentifizierungsmechanismus des bestehenden 802.11b zu verbessern, und die Ergebnisse werden möglicherweise auch als sogenannter 802.1x Standard, eine „Port-Based Network Access Control" (übersetzt: „Anschlussbasierte Netzwerkzugangssteuerung") veröffentlicht, jedoch sind diese Arbeiten noch nicht abgeschlossen. Darüber hinaus berücksichtigt diese Herangehensweise nur eine Authentifizierung, so dass immer noch ein richtiger Geheimhaltungsalgorithmus erforderlich ist. In dieser Hinsicht legen es derzeitige Trends nahe, dass ein auf dem sogenannten Advanced Enryption System (AES)-Protokoll basiertes Protokoll den WEP-Standard ersetzen kann. Nichtsdestotrotz übt der in 802.1x vorgeschlagene "Anschluss-basierte Authentifizierungsmechanismus", einen bedeutenden Einfluss aus auf das TE Betriebssystem und auf die verfügbare Software in den AP's, weil 802.1x nur einen Ersatz für die auf WEP-basierten Authentifizierungsmechanismen und das WEP selbst sucht.

[0011] Kurzfristig wird eine massive Übernahme dieses neuen Standards 802.1x, mit den ganzen nicht gelösten obigen Mängeln zu neuen Investitionen in WLAN Ausrüstung führen, weil durch alle AP's eines gegebenen WLAN ersetzt oder zumindest nachgerüstet werden sollten. Darüber hinaus und einigermaßen offensichtlich stellt jeder WLAN Vertraulichkeitsmechanismus nur einen Schutz auf dem drahtlosen Pfad bereit, d. h. zwischen der WLAN Karte und dem AP. Der entsprechende Ethernet-Verkehr jenseits des AP wird jedoch überhaupt nicht verschlüsselt.

[0012] Es ist daher eine wichtige Aufgabe der vorliegenden Erfindung, in diesem Stadium Mittel und Verfahren bereitzustellen zum Ermöglichen eines effektiven Authentifizierungsmechanismus von WLAN Benutzern und ebenso einen vollständigen Verschlüsselungsmechanismus über den gesamten, bei der Endgerätvorrichtung des Benutzers beginnenden Kommunikationspfads.

Zugehöriger Stand der Technik

[0013] Kurz gesagt und wie oben bereits besprochen ist die Authentifizierung in derzeitigen in WLAN einsetzbaren Standards, nämlich 802.11, entweder nicht existent oder geräte-basiert, wenn die physikalische MAC Adresse der WLAN Karte zur Authentifizierung der TE benutzt wird. Dies ist für große Aufstellungen offensichtlich unbrauchbar, angesichts der Tatsache, dass eine Verschlüsselung, die durch das WEP Protokoll, wie in WLAN, das für seine Schwächen bekannt ist, erreicht wird, von verschiedenen Sektoren als zum Aufrechterhalten einer akzeptablen Sicherheit nicht angemessen befunden wird.

[0014] Im Gegensatz dazu wird die Authentifizierung in herkömmlichen und neueren öffentlichen Landmobilnetzwerken, wie GSM, GPRS oder UMTS, erzielt mittels einer SIM Karte und einem Satz sicherheits-fester Protokolle und Algorithmen, die als „Authentifizierung und Schlüsselübereinkommen" (Englisch: Authentication and Key Agreement (im Folgenden als AKA abgekürzt)-Algorithmen bekannt sind.

[0015] Eine sogenannte SIM-basierte Authentifizierung ist benutzerbasiert, weil eine SIM zur persönlichen Verwendung ausgelegt ist und durch eine Zugangs-PIN geschützt ist.

[0016] Heutzutage möchten Mobilfunkbetreiber ihr Angebot in Zugangsnetzwerken durch das Einschließen von Breitbandzugang erweitern, und die WLAN Technologie macht dies mit Zugangsraten von bis zu 11 Mbps möglich, wobei hauptsächlich durch die Benutzung von nicht lizensiertem Spektrumsband in WLAN extrem niedrige Aufstellungskosten erzielbar sind. Ein Mobilfunkbetreiber kann dies erreichen durch Installieren seines eigenen WLAN oder durch das Zeichnen von Vereinbarungen mit bestehenden WLAN Betreibern, jedoch sollten in beiden Fällen die Sicherheitserfordernisse mindestens so hoch sein wie im Fall eines mobilen Zugangs zum Kernnetzwerk des Betreibers.

[0017] Um dies zu erreichen, muss ein WLAN Betreiber einen Authentifizierungs- und Verschlüsselungsmechanismus anbieten, der den Besitz einer SIM Karte voraussetzt. Diese SIM Karte muss durch den Mobilbetreiber ausgegeben werden und kann dann die gleiche SIM sein wie die, die für mobilen Zugang benutzt wird, oder kann eine SIM sein, die absichtlich nur für WLAN Zugang ausgegeben worden ist.

[0018] Ein von einem Dritten betriebener, herkömmlicher WLAN kann auch seine eigenen lokalen Benutzer aufweisen, und die durch die lokalen Benutzer auszuführende Authentifizierung hängt vollständig vom WLAN Betreiber ab. Beispielsweise kann diese Authentifizierung für lokale Benutzer lediglich auf einer Benutzeridentität plus einem Passwort beruhen, oder sogar überhaupt keine Sicherheit umfasst. Jedoch sollten für diejenigen Benutzer, die bei einem Mobilbetreiber eingeschrieben sind, die Authentifizierung und andere Sicherheitsaspekte durch den WLAN vergleichbar sein mit denjenigen im Netzwerk des Mobilbetreibers. Andererseits sollte ein WLAN,

der nur von einem Mobilfunkbetreiber aufgestellt und betrieben wird, den Zugang verweigern für Benutzer, die nicht zu diesem Mobilbetreiber gehören, und sollte nur auf einer SIM Karte basierende Authentifizierungsmechanismen implementieren.

[0019] Nichtsdestotrotz muss jeglicher Versuch, neue und sichere Mechanismus zur Authentifizierung und Verschlüsselung in WLAN einzuführen, darauf ausgerichtet sein, in derzeitigen WLAN Szenarios so wenig Einfluss wie möglich zu erzeugen.

[0020] Ein ziemlich interessanter Ansatz, zum Lösen des oben beschriebenen Problems ist die Veröffentlichung der Anmeldung US 2002/0009199 mit dem Titel „Data Ciphering in a Wireless Telecomunication System" (übersetzt: "Einrichten von Datenchiffrierung in einem drahtlosen Telekommunikationssystem"). Die dieser Anmeldung zugrunde liegende technische Lehre liefert ebenfalls ein SIM-basiertes Authentifizierungsschema.

[0021] Dieses SIM-basierte Authentifizierungsschema ist jedoch dazu gedacht, einen Chiffrierungsschlüssel, der als der Schlüssel des 802.11 nativen WEP Algorithmus für die Verschlüsselung von Verkehr zwischen der TE und der AP verwendet wird, abzuleiten. Der Hauptvorteil, den diese Anwendung über die bestehenden WEP Fähigkeiten hinaus einführt, ist das Hinzufügen eines neuen Mechanismus zum Erneuern der Schlüssel einmal pro Sitzung. Abgesehen davon ist diese Anwendung hauptsächlich eine modifizierte Version des derzeitigen WEP Standards und löst nicht die oben genannten fundamentellen Probleme für die ursprüngliche WEP Version.

[0022] Nichtsdestotrotz haben verschiedene Sektoren in der Industrie beurteilt, dass wohlbekannte WEP Angriffe einen WEP Schlüssel in weniger als zwei Stunden erraten können. Offensichtlich gilt, dass wenn der WEP Schlüssel statisch ist und niemals erneuert wird, wie in der ursprünglichen WEP Version, das Problem noch viel größer ist. Folglicherweise ist mit dem in US 2002/0009199 dargestellten Ansatz das Problem auf die Begrenzungen der Dauer einer gegebenen Sitzung beschränkt, und wenn sich eine Sitzung über einige Stunden erstreckt, dann tritt das gleiche Problem wie oben auf. Dies ist zum Gewähren von vergleichbaren Sicherheitsniveaus wie die, die in derzeitigen öffentlichen mobilen Landnetzwerken gefunden werden, klar unzureichend.

[0023] In dieser Hinsicht ist eine Aufgabe der vorliegenden Erfindung, ein viel höheres Sicherheitsniveau zu errichten, das es dem Betreiber ermöglicht, einen Verschlüsselungsalgorithmus auszuwählen, der ihre Sicherheitsbedürfnisse besser erfüllt. Es sei angemerkt, dass normalerweise ein Kompromiss zwischen dem Sicherheitsgrad und der Leistungsfähigkeit besteht. Daher können zusätzliche Merkmale, wie etwas das Unterstützen von Schlüsseln mit einer Länge von 128, 168 oder 256 Bits, usw. ebenso wie das Unterstützen der aktuellsten Sicherheitsalgorithmen, wie z. B. etwa AES, sowie eine Schlüsselrotationsprozedur als weitere Aufgaben der vorliegenden Erfindung betrachtet werden.

[0024] Ferner geht gemäß der oben genannten Anmeldung (US 2002/0009199) der verschlüsselte Pfad von dem mobilen Endgerät zur AP, weil WEP nur auf dem Funkpfad anwendbar ist. In dieser Hinsicht sind die Unterstützung eines über den AP hinaus zu errichtenden Verschlüsselungspfads und das Überdecken auch des drahtgestützten Teils des WLANs weitere Aufgaben der vorliegenden Erfindung.

[0025] Ferner lehrt die US 2002/0009199, dass die Zuordnung einer IP Adresse ausgeführt wird, bevor der Authentifizierungsprozess durchgeführt wird, und folglich kann ein böswilliger Benutzer möglicherweise eine ganze Menge wohlbekannter Angriffe initiieren. Wenn jedoch ein Benutzer keine Mittel hatte, um die IP Verbindungsfähigkeit zu erlangen, bevor er effektiv authentifiziert ist, würde das Risiko stark abnehmen. Folglich ist eine weitere Aufgabe der vorliegenden Erfindung die Bereitstellung eines Authentifizierungsmechanismus für einen Benutzer, der auszuführen ist, bevor dem Benutzer die IP Verbindungsfähigkeit gegeben wird.

[0026] Andererseits offenbaren die Anmeldungen US 2002/012433 und WO 01/76297 anhand einiger üblicher beispielhafter Ausführungsformen ein System, in dem sich ein drahtlos angepasstes Endgerät mit einem mobilen Heimatnetzwerk über ein drahtloses IP Zugangsnetzwerk verbinden kann. Das mobile Heimatnetzwerk ist für die Authentifizierung des Benutzers mit einer SIM-basierten Authentifizierung verantwortlich, wohingegen das drahtlose IP Zugangsnetzwerk dem Benutzer erlaubt, auf das Internetnetzwerk zuzugreifen, sobald er authentifiziert ist. Das drahtlose Endgerät, das drahtlose IP Zugangsnetzwerk und das mobile Netzwerk kommunizierten alle mit einem mobilen IP Protokoll. Das System umfasst auch eine Steuereinheit für öffentlichen Zugang (Englisch: PAC Public Access Controller) zum Steuern des Zugangs aus dem Funkzugangsnetzwerk zu den Internetdiensten. Diese Steuereinheit für öffentlichen Zugang stellt dem drahtlosen Endgerät eine IP Adresse bereit und authentifiziert das drahtlose Endgerät, bevor eine Verbindung mit dem Internet errichtet ist, und leitet Authentifizierungsnachrichten zwischen dem drahtlosen Endgerät und dem mobilen Heimatnetzwerk weiter. Ferner ist die Schnittstelle zwischen dem drahtlosen Endgerät und der öffentlichen Zugangssteuereinheit eine IP basierte Schnittstelle, wobei die Steuereinheit für öffentlichen Zugang und das drahtlose Endgerät durch entsprechende IP Adressen vor einander identifiziert werden. Die Tatsache, dass die Steuereinheit für öffentli-

chen Zugang und das drahtlose Endgerät ein IP-basiertes Protokoll benutzen, macht es wesentlich, dass dem drahtlosen Endgerät von Anfang an eine IP Adresse zugewiesen wird, wobei diese IP Adresse von der Steuereinheit für öffentlichen Zugang an das drahtlose Endgerät vor dem Errichten einer sicheren Kanalkommunikation gesendet wird. Dabei tritt aufgrund der Tatsache, dass die Zuweisung einer IP Adresse vor dem Ablaufen des Authentifizierungsprozesses ausgeführt wird, das gleiche Problem auf wie bei der obigen Anmeldung (US 2002/009199) und folglich kann ein böswilliger Benutzer möglicherweise eine ganze Menge wohlbekannter Angriffe initiieren.

[0027] Zusammenfassend ist eine wichtige Aufgabe der vorliegenden Erfindung die Bereitstellung eines Systems, von Mitteln und Verfahren zum Ermöglichen einer effektiven, SIM-basierten Benutzerauthentifizierung und zum Errichten eines vollständigen Verschlüsselungspfads, beginnend bei der TE, für WLAN Benutzer, die Teilnehmer eines öffentlichen Landmobilnetzwerks sind. Eine andere besonders wichtige Aufgabe ist, dass diese SIM-basierte Benutzerauthentifizierung ausgeführt werden kann, bevor dem Benutzer die IP Verbindungsfähigkeit verliehen wird.

[0028] Eine weitere Aufgabe der vorliegenden Erfindung ist die Unterstützung von Schlüsseln mit variabler Länge, die Benutzung von Sicherheitsalgorithmen zur Auswahl durch den Betreiber sowie die Bereitstellung eines Schlüsselrotationsverfahrens.

[0029] Einen noch weitere Aufgabe der vorliegenden Erfindung ist das Erreichen der vorgenannten Ziele mit einem minimalen Einfluss auf herkömmliche WLAN Szenarien.

Zusammenfassung der Erfindung

[0030] Die Aufgaben der Erfindungen werden gelöst durch ein Verfahren zum Erlauben einer SIM-basierten Authentifizierung für Benutzer eines drahtlosen Lokalnetzwerks, die Teilnehmer eines öffentlichen Landmobilfunknetzes sind, mittels Datenverbindungsschicht (Englisch: Data Link Lager) Schicht-2 (Englisch: Lager-2) Authentifizierungsmechanismus. Ein wichtiger Aspekt dieses Verfahrens ist, dass die IP Verbindungsfähigkeit dem Benutzer nur dann bereitgestellt wird, wenn der Authentifizierungsprozess erfolgreich abgeschlossen ist. Die Aufgaben der Erfindung werden daher erreicht mit einem Verfahren, bei dem ein drahtloses Endgerät einen zugänglichen Zugangspunkt findet und die Assoziierung mit dem drahtlosen Lokalnetzwerk anfragt, und der Zugangspunkt die Anfrage dafür akzeptiert. Das drahtlose Endgerät initiiert dann das Auffinden einer Zugangssteuereinheit, die zwischen dem Zugangspunkt und dem öffentlichen Landmobilfunknetz zwischengeschaltet ist.

[0031] Dann sendet das drahtlose Endgerät den Benutzerbezeichner unmittelbar auf ein Schicht-2 Punkt-zu-Punkt Protokoll (Englisch: Point-to-point Lager 2 protocol) gerichtet an die Zugangssteuereinheit, die dann in oben auf einem Schicht-2 Punkt-zu-Punkt Protokoll empfangenen Benutzerkennzeichner aufwärts an ein in der Anwendungsebene angesiedeltes Authentifizierungsprotokoll weitergibt.

[0032] Danach sendet die Zugangssteuereinheit den Benutzerkennzeichner gerichtet an einen Authentifizierungs-Gateway in dem öffentlichen Landmobilfunknetz, um einen Authentifizierungsvorgang zu initiieren.

[0033] Nachdem der Authentifizierungsvorgang gestartet ist, empfängt die Zugangssteuereinheit eine Authentifizierungsanfrage von dem öffentlichen Landmobilfunknetz über den Authentifizierungs-Gateway; und verschiebt die von demselben Protokoll auf der Anwendungsebene empfangene Authentifizierungsanfrage abwärts oben auf das Schicht-2 Punkt-zu-Punkt Protokoll. Die Authentifizierungsanfrage wird von der Zugangssteuereinheit gerichtet an das drahtlose Endgerät gesendet, um eine Authentifizierungsanfrage abzuleiten.

[0034] Dann kann das drahtlose Endgerät die Authentifizierungsantwort unmittelbar oben auf ein Schicht-2 Punkt-zu-Punkt Protokoll gerichtet an die Zugangssteuereinheit senden, die die oben auf dem Schicht-2 Punkt-zu-Punkt Protokoll empfangene Authentifizierungsantwort aufwärts zu dem Authentifizierungsprotokoll in der Anwendungsebene verschiebt. Die Authentifizierungsantwort wird von der Zugangssteuereinheit, die einen Verschlüsselungsschlüssel von dem öffentlichen Landmobilnetzwerk über den Authentifizierungs-Gateway empfängt, gerichtet an den Authentifizierungs-Gateway gesendet.

[0035] Danach extrahiert die Zugangssteuereinheit den auf dem Protokoll in der Anwendungsebene empfangenen Verschlüsselungsschlüssel zur weiteren Verschlüsselung des Kommunikationspfads mit dem drahtlosen Endgerät; und die Zugangssteuereinheit sendet eine zugewiesene IP Adresse und andere Netzwerkkonfigurationsparameter gerichtet an das drahtlose Endgerät.

[0036] Dies stellt den Vorteil bereit, dass das mobile Endgerät im gesamten Kommunikationspfad einen Sicherheitsauthentifizierungsmechanismus, ähnlich den in Funkkommunikationsnetzwerken benutzten, hinzufügt, was bedeutet, dass die Geheimhaltung im drahtlosen Pfad und im drahtgestützten Pfad erzielt wird. Die Betreiber können ihre Zugangsnetzwerke erweitern, in dem sie lokalisierten Breitbandzugang

(11 Mbps) bei sehr niedrigen Kosten anbieten.

[0037] Auch wird zum Erreichen der Aufgaben der vorliegenden Erfindung eine Zugangssteuereinheit mit einem in einer OSI Schicht-2 angeordneten Punkt-zu-Punkt Server bereitgestellt zum Kommunizieren mit dem drahtlosen Endgerät; und ein in einer OSI Anwendungsebene angesiedeltes Authentifizierungsprotokoll zum Kommunizieren mit dem öffentlichen Landmobilfunknetz. Darüber hinaus umfasst diese Zugangssteuereinheit auch ein Mittel zum Schieben der oben auf dem Schicht-2 Punkt-zu-Punkt Protokoll empfangenen Information aufwärts zu einem geeigneten, in der Anwendungsebene angesiedelten Authentifizierungsprotokoll. In ähnlicher Weise umfasst auch die Zugangssteuereinheit Mittel zum Schieben der oben auf dem in der Anwendungsebene residierenden Authentifizierungsprotokoll empfangenen Information abwärts nach oben auf das Schicht-2 Punkt-zu-Punkt Protokoll.

[0038] Um die Aufgaben der vorliegenden Erfindung vollständig zu erzielen, wird auch ein drahtloses Endgerät bereit gestellt, das Funktionalität bereit stellt zum Agieren als eine Schicht-2 Punkt-zu-Punkt Protokoll-Client und das oben auf diesem Schicht-2 Punkt-zu-Punkt Protokoll ein erweiterbares Authentifizierungsprotokoll aufweist.

[0039] Die durch die Erfindung bereit gestellte Gesamtlösung resultiert in einem Telekommunikationssystem, das folgendes umfasst: ein drahtloses Lokalnetzwerk mit mindestens einem Zugangspunkt, ein öffentliches Landmobilfunknetz, mindestens ein drahtloses Endgerät wie oben, und die obige Zugangssteuereinheit.

Kurze Beschreibung der Zeichnungen

[0040] Die Merkmale, Aufgaben und Vorteile der Erfindung werden offensichtlich durch Lesen dieser Beschreibung zusammen mit den beigefügten Zeichnungen, für die gilt:

[0041] Fig. 1 stellt eine bevorzugte Ausführungsform davon dar, wie ein Benutzer eines herkömmlichen Mobilfunknetzes, der durch ein WLAN, auf das von mobilen und nicht mobilen Benutzern zugegriffen werden kann, Zugang erlangt, durch sein eigenes Mobilfunknetz authentifiziert werden kann und einen verschlüsselten Pfad von dem TE zu seinem eigenen Mobilfunknetzwerk zur Verfügung gestellt bekommen.

[0042] Fig. 2 zeigt eine im Vergleich zu der Architektur in Fig. 1 vereinfachte Architektur, die auf einen WLAN, auf den nur Benutzer eines öffentlichen Landmobilfunknetzes zugreifen, anwendbar ist.

[0043] Fig. 3 zeigt schematisch eine Ausführungsform einer Zugangssteuereinheit mit einem PPPoE Server und einem RADIUS Client, in dem sich das erweiterbare Authentifizierungsprotokoll angeordnet ist.

[0044] Fig. 4 zeigt im Wesentlichen eine beispielhafte Abfolge von Aktionen, die von dem TE zu dem Mobilfunknetz und durch die WLAN Einheiten hindurch ausgeführt werden, um eine SIM-basierte Benutzerauthentifizierung auszuführen.

Ausführliche Beschreibung bevorzugter Ausführungsformen

[0045] Das Folgende beschreibt derzeit bevorzugte Ausführungsformen von Mitteln, Verfahren und ein System zum Ermöglichen einer effektiven, SIM-basierten Benutzerauthentifizierung und zum Errichten eines vollständigen Verschlüsselungspfads beginnend bei der TE für WLAN Benutzer, die Teilnehmer eines öffentlichen Landmobilfunknetzes sind. Nach einem Aspekt der vorliegenden Erfindung wird diese SIM-basierte Benutzerauthentifizierung ausgeführt bevor dem Benutzer eine IP Verbindungsfähigkeit verliehen worden ist.

[0046] Daher wird in Fig. 1 eine Gesamtskizze einer bevorzugten Ausführungsform vorgestellt. Diese zeigt ein allgemeines Szenario, bei dem Teilnehmer eines öffentlichen Landmobilfunknetzes (GSM/GPRS/UMTS) ebenso wie andere lokale, nicht mobile Benutzer, auf ein drahtloses Lokalnetzwerk (WLAN) zugreifen. Dieses allgemeine Szenario in Fig. 1 schlägt eine besonders einfache Architektur vor, die darauf abzielt, die Einflüsse auf ein bestehendes herkömmliches WLAN zu minimalisieren, um eine der Aufgaben der vorliegenden Erfindung zu lösen. Diese ziemlich einfache Architektur bezieht verschiedene, im Folgenden beschriebene Einheiten aus einem WLAN und aus einem öffentlichen Landmobilfunknetz mit ein. Ferner gibt Fig. 2 eine noch weiter vereinfachte Architektur gemäß einer anderen Ausführungsform der vorliegenden Erfindung für ein WLAN ohne lokale WLAN Benutzer, das nur an Teilnehmer eines öffentlichen Landmobilfunknetzes Zugang verleiht.

[0047] Eine erste Einheit in Fig. 1 und Fig. 2 ist die Endgeräteapparatur (TE, Englisch: Terminal Equipment), die mit der notwendigen Hardware und Software zum Dienen als Schnittstelle mit der SIM Karte des Benutzers und ebenso zum Senden und Empfangen der erforderlichen Benachrichtigungsinformation nach der Authentifizierungs- und Schlüsselübereinkunft (AKA, Englisch: Authentication and Key Agreement)-Protokoll ausgerüstet ist. Die TE umfasst auch die erforderliche Software, um ein Punkt-zu-Punkt Protokoll über Ethernet (PPPoE) Protokoll, Clientseitig und gemäß RFC 2516 zu implementieren.

[0048] Das Einschließen eines derartigen PPPoE Client ermöglicht die Errichtung einer Punkt-zu-Punkt Protokoll (PPP) Sitzung mit einem bestimmten Server in der WLAN Domäne. Dies ist eine sehr günstige Ausführungsform, um bestehenden Authentifizierungsmechanismen zum Durchbruch zu verhelfen, beispielsweise dem erweiterbaren Authentifizierungsprotokoll (EAP, Englisch: Extensible Authentication Protocol) und Verschlüsselungsprotokollen, wie etwa dem PPP Verschlüsselungssteuerungsprotokoll (im folgenden als „PPP verschlüsselt" bezeichnet) gemäss RFC 1968, das den Verschlüsselungspfad entlang des drahtgestützten Teils des WLAN erweitert, was ein viel höheres Sicherheitsniveau bietet. Eine Komponente wie dieser PPPoE Client ist ein Kernelement für die vorgeschlagene Lösung.

[0049] Andere Einheiten in den Szenarien der Fig. 1 und Fig. 2 sind die Zugangspunkte (AP), die sich als reine Standardfunkstationen gemäss dem Standard 802.11b ohne jegliche zusätzliche Logik verhalten. Anders als andere mögliche Lösungen, wie bezüglich des aufkommenden Standards 802.1x erläutert, erlaubt der durch die vorliegende Erfindung angebotene Ansatz die Wiederverwendung der bestehenden preiswerten Hardware anstatt dass alle in den WLAN vorhandenen AP's (Englisch: Access Point) ersetzt oder nachgerüstet werden müssen. Diese unveränderten AP's können in diesem Szenario mit dem ausgeschalteten WEP Support laufen gelassen werden, weil ein derartiger WEP aus sich selbst heraus eine geringere Sicherheit als im Vergleich zu den oben auf der PPPoE Ebene implementierten Sicherheitsmechanismen bietet.

[0050] Nach einem Aspekt der vorliegenden Erfindung wird eine neue Einheit bereitgestellt, die Zugangssteuereinheit (im Folgenden als AC, Englisch: Access Controller) sowohl in Fig. 1 als auch in Fig. 2 bereitgestellt, welche AC die erforderliche PPPoE Serverfunktionalität umfasst. Dieser PPPoE Server wird von der Endgeräteapparatur (TE) automatisch durch einen eingebauten Mechanismus in dem PPPoE Protokoll erkannt, nämlich durch einen Handshake, der durch eine als Sammelruf ausgesendete Nachricht initiiert wurde. Diese Zugangssteuereinheit (AC) umfasst auch eine Funktionalität als RADIUS Client, die die Verantwortlichkeit aufweist für das Einholen von Client-Berechtigungsnachweisen, die durch oben auf einem PPP getragenen EAP Attributen empfangen werden, und für das Aussenden derselben gerichtet an einen herkömmlichen WLAN Authentifizierungsserver (WLAN-AS), und auch durch EAP Attribute, die oben auf RADIUS Nachrichten getragen werden. Eine Komponente wie diese Zugangssteuereinheit (AC), ist auch ein Kernelement für den Zweck der vorliegenden Lösung.

[0051] Sowohl die Zugangssteuereinheit als auch der vorgenannte, in der Endgeräteapparatur eingebettete PPPoE Client sind kooperierende Einheiten, die zum Tunneln einer Anfrage/Antwort-Authentifizierungsprozedur ebenso wie zum Errichten eines verschlüsselten Pfads gedacht sind.

[0052] Eine weitere nur in dem in Fig. 1 gezeigten Allgemeinszenario vorhandene Einheit ist ein WLAN-Authentifizierungsserver (WLAN-AS), der die Funktionalität eines lokalen Authentifizierungsservers implementiert für nicht zu dem Mobilbetreiber gehörende, lokale WLAN Benutzer, die folglich durch andere Mittel, wie etwa eine reine Benutzer- und Passwortanpassung authentifiziert werden können. Dieser WLAN-AS spielt auch die Rolle eines RADIUS Proxy, wenn Authentifizierungsnachrichten von der Zugangssteuereinheit empfangen werden, und leitet diese gerichtet an einen Authentifizierungs-Gateway (im folgenden als AG bezeichnet) weiter in der Domäne des Betreibers des öffentlichen Landmobilfunknetzes.

[0053] Der WLAN-AS ist nur erforderlich für den Zweck der vorliegenden Erfindung, um die eigenen WLAN Benutzer, die keine mobilen Teilnehmer des öffentlichen Landmobilfunknetzes sind, zu authentifizieren. Folglich kann ein WLAN, das zum Verleihen von Zugang nur an Teilnehmer eines Mobilfunknetzes gedacht ist, sich von derartigen Einheiten befreien, ohne die Authentifizierung des mobilen Teilnehmers und die Errichtung eines verschlüsselten Pfads zu beeinflussen, was der Umfang der vorliegenden Erfindung ist. In dieser Hinsicht zeigt Fig. 2 eine Ausführungsform einer vereinfachten Architektur für ein WLAN, das Zugang nur an Teilnehmer eines öffentlichen Landmobilfunknetzes, in dem der WLAN-AS folglich nicht enthalten ist wie oben erläutert, verleiht.

[0054] Eine noch weitere in den Szenarien der Fig. 1 und Fig. 2 enthaltene Einheit ist der Authentifizierungs-Gateway (im Folgenden als AG bezeichnet), allein oder wahrscheinlich in Kooperation mit einem Heimatortregister (HLR, Englisch: Home Location Register) zum Speichern der Benutzerdaten von mobilen Teilnehmern. Dieser Authentifizierungs-Gateway (AG), alleine oder in Kombination mit einem HLR, fungiert als Backend-Server zur Authentifizierung innerhalb der Domäne des Betreibers, und betreut das Erzeugen von Authentifizierungsvektoren nach dem AKA Protokoll für herkömmliche und neuere öffentliche Landmobilfunknetze, wie etwa GSM, GPRS und UMTS. Diese Komponenten, nämlich AG und HLR, können physikalisch getrennte Einheiten sein, die miteinander durch das mobile Anwendungsteil (MAP, Englisch: Mobile Application Part)-Protokoll miteinander kommunizieren, oder sie können eine einzelne logische Einheit sein, die als ein RADIUS Server mit eingebauter Teilnehmerdatenbank, zusammen mit der Implementierung der erforderlichen Algorithmen in AKA, wie etwa die wohl bekannten A5, A8 usw., agiert. Im letzteren Ansatz ist die Kommuni-

kation in Richtung auf einen HLR folglich nicht erforderlich, wie beispielhaft in Fig. 2 veranschaulicht.

[0055] Kurz gesagt sind die Zugangssteuereinheit, der vorgenannte, in der Endgeräteapparatur eingebettete PPPoE Client und dieser Authentifizierungs-Gateway die Kerneinheiten für den Zweck der vorliegenden Erfindung. Die besondere Beschreibung der in diesen Einheiten vorhandenen Funktionen geschieht nur veranschaulichend und in einer nicht beschränkenden Weise.

[0056] Fig. 3 zeigt verschiedene in einer Zugangssteuereinheit (AC) involvierte Protokollebenen mit Verweis auf das Modell der systemunabhängigen Kommunikation (OSI, Englisch: Open System Interconnection). Der unterhalb einer IP Ebene angeordnete PPPoE Server umfasst eine PPPoE Protokollebene, die natürlicherweise über einer Ethernetebene residiert, und weist die den vorgenannten eingebetteten EAP auf. In ähnlicher Weise gilt, dass der RADIUS Client eine RADIUS Protokollschicht aufweist, die die EAP eingebettet aufweist, wobei die EAP über einem UDP Layer angesiedelt ist, die beide über einer IP Ebene angesiedelt sind.

[0057] Andererseits wird die Art und Weise, in der die verschiedenen Elemente einiger Aspekte die vorliegende Erfindung gemäß den derzeit bevorzugten Ausführungsformen ausführen, im Folgenden mit Verweis auf die Abfolge der in Fig. 4 gezeigten Aktionen beschrieben.

[0058] Die vorgenannte Endgeräteapparatur (TE) ist mit einem Mobilfunkendgeräteadapter (MTA, Englisch: Mobile Terminal Adapter), der den Zugriff auf eine in dem Mobilfunkendgerät getragenen SIM Karte erlaubt, ausgerüstet. Diese TE weist ein Sendeempfangsgerät auf zum Kommunizieren (C-401, C-402) mit einem AP des WLAN, und umfasst den geeigneten Software-Stapel, um das PPPoE Protokoll gemass RFC 2516 zu implementieren.

[0059] Die Zugangssteuereinheit (AC) weist einen eingebetteten PPPoE Server auf. Das Erkennen des PPPoE Servers durch den PPPoE Client ist ein integraler Teil des Protokolls selbst (C-403, C-404, C-405, C-406). Die von dem TE auf der PPPoE Verbindung (C-407, C-408) benutzte Identität ist ein Netzwerkzugangsbezeichner (NAI, Englisch: Network Access Identifier), der vom Benutzer eingegeben wird, um die erforderlichen Einwahlsitzungen herzustellen, und dessen Wirkungsbereich benutzt wird, um den Benutzer als einen Teilnehmer eines gegebenen Mobilbetreibers zu identifizieren. Es wird kein Passwort benötigt, weil die Authentifizierung durch andere Mittel ausgeführt wird. Alternativ könnte die IMSI anstelle des Sendens einer NAI von der SIM Karte geholt werden und als die Benutzeridentität gesendet werden. Dies sollte nur eingesetzt werden, wenn das Aussenden der IMSI im Klartext akzeptabel ist, was nicht der Fall sein könnte.

[0060] Nachdem die Benutzeridentität mit Hilfe des EAP Mechanismus empfangen worden ist, weist die Zugangssteuereinheit (AC) einen RADIUS Client auf zum Senden (C-408) von Authentifizierungsnachrichten an den WLAN-AS Server. Das erweiterbare Authentifizierungsprotokoll (EAP) wird oben auf PPP und RADIUS ablaufen gelassen, um Authentifizierungsinformation zwischen der TE und der AG zu transportieren. Der innerhalb der EAP zu benutzende Authentifizierungsmechanismus kann der gewöhnliche, in öffentlichen Landmobilfunknetzen benutzte AKA sein. Wie bereits oben erwähnt, fungiert der WLAN-AS als ein Authentifizierungsserver für reguläre WLAN Benutzer, deren Authentifizierung nicht SIM-basiert ist, und als ein Authentifizierungs-Proxy für diejenigen Benutzer, deren Bereichsteil der NAI diese als Teilnehmer eines Mobilfunknetzes identifiziert, wodurch eine SIM-basierte Authentifizierung eingesetzt wird. Wenn er dann als ein Authentifizierungs-Proxy fungiert, leitet der WLAN-AS (C-410) die empfangenen Authentifizierungsnachrichten an den Authentifizierungs-Gateway (AG) weiter.

[0061] Wenn der Authentifizierungs-Gateway eine Authentifizierungsanforderung empfängt, fragt die HRL unter Benutzung einer MAP Schnittstelle nach einem Authentifizierungsvektor (C-411), Trielet oder Quintet. Für diese Aufgabe muss der Authentifizierungs-Gateway (AG) die IMSI des Teilnehmers, dessen NAI in der RADIUS Nachricht gesendet worden sind, kennen. Diese IMSI kann beispielsweise durch ein Nachschlagen in einer Verzeichnisdatenbank erkannt werden. Die HLR antwortet mit der angeforderten Authentifizierungsinformation (C-412) für den Benutzer.

[0062] Dann kapselt die AG die RAND Komponente des Authentifizierungsvektors in ein EAP Attribut und sendet dies innerhalb einer RADIUS Nachricht durch den WLAN-AS (C-413) gerichtet an den AC (C-414) zurück. Es sei angemerkt, dass für Benutzer von neueren mobilen Netzwerken, wie etwa UMTS, auch das Aussenden einer Nachricht wie etwa AUTN erforderlich sein kann.

[0063] Die AC leitet dann (C-415) die empfangene EAP Information in einer PPP Nachricht an die PE weiter. Es sei angemerkt, dass die AC sich hier als ein „Durchlauf" der EAP Information zwischen „Carrier" Protokollen, wie etwa PPP und RADIUS, verhält.

[0064] Wenn die TE die EAP Information empfängt, die RAND Nummer extrahiert und diese benutzt, um die SIM abzufragen und eine Antwort (RES) zu erzeugen, die dann an die AG über das wiederum über PPP und RADIUS übertragene EAP zurückgeschickt wird (C-416, C-417, C-418). Wie zuvor für UMTS Be-

nutzer authentifiziert die TE zuerst das Netzwerk, basiert auf der AUTN. Bei diesem Schritt ist anzumerken, dass die TE den Verschlüsselungsschlüssel erzeugt, und zwar gemäß dem im AKA definierten Standardalgorithmus. Dieser Schlüssel wird als ein Keim, nämlich als Verschlüsselungsmaterial, benutzt, um einen oder mehrere, mit dem in RFC 1968 genannten PPP Verschlüsselungssteuerungsprotokoll und ebenso mit den bestehenden PPP Verschlüsselungsalgorithmen zu benutzende Sitzungsschlüssel, beispielsweise das PPP Triple-DES Verschlüsselungsprotokoll, RFC 2420, abzuleiten.

[0065] Die AG empfängt (C-418) die EAP Antwort und überprüft die Gültigkeit der Anfrage. Der AKA Verschlüsselungsschlüssel (Kc) wurde vorher in dem Authentifizierungsvektor von der HLR, wahrscheinlich in Kooperation mit einem nicht gezeigten Authentifizierungszentrum (AuC, Englisch: Authentication Centre) empfangen. Die AG kommuniziert dann den AKA Verschlüsselungsschlüssel (Kc) an den AC (C-419, C-420), wo der PPPoE Server residiert. Dies kann in einer RADIUS Zugangsakzeptierungs-(Englisch: Access Accept) Nachricht ausgeführt werden, in der der EAP-Erfolg (Englisch: EAP-Success) übertragen wird, jedoch weil dieser EAP Befehl keine zusätzlichen Daten tragen kann, kann ein RADIUS Anbieterspezifisches Attribut (VSA, Englisch: Vendor Specific Attribute) eine nützlichere Option sein.

[0066] An dieser Stufe empfängt der AC (C-420) eine RADIUS Zugangsakzeptierungsnachricht und fordert eine IP Adresse aus einem dynamischen Host Konfigurationsprotokoll (DHCP, Englisch: Dynamic Host Configuration Protocol) Server, wobei diese IP Adresse weiter an die TE zu senden ist, an. Die AC folgt dem gleichen Algorithmus wie die TE, um aus dem mit dem PPP Verschlüsselungssteuerungsprotokoll und dem gewählten PPP Verschlüsselungsalgorithmus (beispielsweise 3DES) zu benutzenden AKA Verschlüsselungsschlüssel (Kc) Sitzungsschlüssel abzuleiten. Der AC sendet (C-421) möglicherweise die Nachricht „EAP-Erfolg" an die TE, zusammen mit anderen an die TE bestimmten Konfigurationsparametern, wie etwa einer IP Adresse, einer IP Netzmaske, DNS Servern, usw. Dann ist die PPP Verbindung vollständig eingerichtet und dazu bereit, in die Netzwerkphase einzutreten.

Patentansprüche

1. Ein Verfahren in einem Telekommunikationssystem zum Erlauben einer SIM-basierten Authentifizierung für Benutzer eines drahtlosen, lokalen Netzwerks, wobei die Benutzer Teilnehmer eines öffentlichen Landmobilfunknetzes sind, das Verfahren umfassend die folgenden Schritte:
(a) ein drahtloses Endgerät greift über einen zugänglichen Zugangspunkt auf das drahtlose lokale Netzwerk zu;
(b) Erkennen einer zwischen dem Zugangspunkt und dem öffentlichen Landmobilfunknetz des drahtlosen Endgeräts zwischengeschalteten Zugangssteuereinheit;
(c) Ausführen einer SIM-basierten Authentifizierungsprozedur mittels Anfrage/Antwort zwischen dem drahtlosen Endgerät und dem öffentlichen Landmobilfunknetz über die Zugangssteuereinheit, wobei das drahtlose Endgerät mit einer SIM Karte ausgestattet ist und zum Lesen von deren Daten ausgebildet ist;
das Verfahren **dadurch gekennzeichnet**, dass die Einsendungen im Rahmen der Authentifizierung mittels Anfrage/Antwort in Schritt c) stattfinden, bevor eine IP Verbindungsfähigkeit mit dem Benutzer bereitgestellt worden ist, und ausgeführt werden:
– oben auf einem Protokoll der Punkt-zu-Punkt Ebene 2 (PPPoE) (Englisch: Point-to-Point layer 2 protocol) zwischen dem drahtlosen Endgerät und der Zugangssteuereinheit; und
– auf einem sich auf der Anwendungsebene zwischen dem öffentlichen Landmobilfunknetz und der Zugangssteuereinheit befindlichen Authentifizierungsprotokoll; und
das Verfahren ferner einen Schritt umfasst:
(d) dem Benutzer am drahtlosen Endgerät Anbieten von einer IP Verbindungsfähigkeit mit durch Senden einer zugewiesenen IP Adresse und anderen Netzwerkkonfigurationsparametern, wenn der Benutzer einmal von dem öffentlichen Landmobilfunknetzwerk gültig authentifiziert worden ist.

2. Das Verfahren nach Anspruch 1, wobei der Schritt b) des Erkennens einer Zugangssteuereinheit einen Schritt umfasst des Einrichtens einer Arbeitssitzung eines Punkt-zu-Punkt Protokolls zwischen einem Client eines Punkt-zu-Punkt über Ethernet (PPPoE) Protokolls in dem drahtlosen Endgerät und einem Server eines Punkt-zu-Punkt über Ethernet (PPPoE) Protokolls in der Zugangssteuereinheit.

3. Das Verfahren nach Anspruch 1, wobei der Schritt c) des Ausführens der Authentifizierungsprozedur über Anfrage/Antwort die folgenden Schritte umfasst:
(c1) Senden eines Nutzerbezeichners aus dem drahtlosen Endgerät an das öffentliche Landmobilfunknetz über die Zugangssteuereinheit;
(c2) Empfangen einer Authentifizierungsanfrage aus dem öffentlichen Landmobilfunknetz über die Zugangssteuereinheit an dem drahtlosen Endgerät;
(c3) bei dem drahtlosen Endgerät aus der empfangenen Nachricht Ableiten eines Verschlüsselungsschlüssels und einer Authentifizierungsanfrage;
(c4) Senden der Authentifizierungsantwort aus dem drahtlosen Endgerät an das öffentliche Landmobilfunknetz über die Zugangssteuereinheit;
(c5) Empfangen eines Verschlüsselungsschlüssels aus dem öffentlichen Landmobilfunknetz an der Zugangssteuereinheit; und

(c6) Extrahieren des Verschlüsselungsschlüssels, der zur weiteren Verschlüsselung eines Kommunikationspfades mit dem drahtlosen Endgerät empfangen worden ist.

4. Das Verfahren nach Anspruch 2, ferner umfassend einen Schritt des Verschiebens von oben auf einem Protokoll der Punkt-zu-Punkt Ebene 2 (PPPoE) empfangener Authentifizierungsinformation, aufwärts zu einem sich in einer Anwendungsebene für Einsendungen zu dem öffentlichen Landmobilfunknetz befindlichen Authentifizierungsprotokoll.

5. Das Verfahren nach Anspruch 4, ferner umfassend einen Schritt des Verschiebens von auf einem in der Anwendungsebene angeordneten Authentifizierungsprotokoll empfangenen Authentifizierungsinformation, abwärts nach oben auf ein Protokoll einer Punkt-zu-Punkt Ebene 2 (PPPoE) für Einsendungen zu dem drahtlosen Endgerät.

6. Das Verfahren nach Anspruch 3, ferner umfassend einen Schritt des Einrichtens an dem drahtlosen Endgerät eines symmetrischen Verschlüsselungspfads unter Benutzung des zuvor abgeleiteten Verschlüsselungsschlüssels bei der Zugangssteuereinheit und dem drahtlosen Endgerät.

7. Das Verfahren nach einem der vorhergehenden Ansprüche, wobei der Schritt d) des Aussendens einer IP Adresse einen vorhergehenden Schritt des Anfragens einer derartigen IP Adresse von einem Protokollserver für eine dynamische Host-Konfiguration enthält.

8. Das Verfahren nach einem der vorhergehenden Ansprüche, wobei die Kommunikation zwischen der Zugangssteuereinheit und dem öffentlichen Landmobilfunknetz über einen Authentifizierungs-Gateway des öffentlichen Landmobilfunknetzes verläuft.

9. Das Verfahren nach einem der vorhergehenden Ansprüche, wobei die Kommunikation zwischen der Zugangssteuereinheit und dem Authentifizierungs-Gateway eines öffentlichen Landmobilfunknetzes über einen Authentifizierungsserver des für die Authentifizierung von lokalen Benutzern des drahtlosen lokalen Netzwerks, die keine mobilen Teilnehmer sind, zuständigen drahtlosen lokalen Netzes erfolgt.

10. Das Verfahren nach einem der vorhergehenden Ansprüche, wobei der Benutzerkennzeichner in Schritt c1) einen Netzzugangsbezeichner umfasst.

11. Das Verfahren nach einem der vorhergehenden Ansprüche, wobei der Benutzerbezeichner in Schritt c1) eine internationale Mobilteilnehmeridentität umfasst.

12. Das Verfahren nach einem der vorhergehenden Ansprüche, wobei das in der Anwendungsebene im Schritt c) angeordnete Authentifizierungsprotokoll ein erweiterbares Authentifizierungsprotokoll ist.

13. Das Verfahren nach Anspruch 12, wobei dieses erweiterbare Authentifizierungsprotokoll über ein RADIUS-Protokoll transportiert wird.

14. Das Verfahren nach Anspruch 12, wobei das erweiterbare Authentifizierungsprotokoll über ein Durchmesser-Protokoll (Englisch: Diameter Protocol) transportiert wird.

15. Eine Zugangssteuereinheit in einem Telekommunikationssystem, das ein drahtloses Lokalnetzwerk mit mindestens einem Zugangspunkt, ein öffentliches Landmobilfunknetz und mindestens eine mit einer SIM Karte versehene und zum Lesen von deren Teilnehmerdaten ausgebildete Endgerätapparatur umfasst; wobei die Zugangssteuereinheit dadurch gekennzeichnet ist, dass sie umfasst:
(a) einen Server für ein Protokoll einer Punkt-zu-Punkt Ebene 2 (PPPoE) (Englisch: Point-to-Point layer 2 protocol) zum Kommunizieren mit dem drahtlosen Endgerät, und ausgebildet zum Durchtunneln des SIM-basierten Authentifizierungsprotokolls mittels Anfrage/Antwort; und
(b) ein Authentifizierungsprotokoll, das auf einer OSI Anwendungsebene zum Kommunizieren mit dem öffentlichen Landmobilfunknetz angeordnet ist.

16. Die Zugangssteuereinheit nach Anspruch 15, ferner umfassend:
(a) Mittel zum Verschieben der auf der Oberseite des Protokolls der Punkt-zu-Punkt Ebene 2 (PPPoE) empfangenen Information aufwärts zu dem in der Anwendungsschicht angeordneten Authentifizierungsprotokoll; und
(b) Mittel zum Verschieben der auf dem in der Anwendungsebene angeordneten Authentifizierungsprotokoll empfangenen Information abwärts nach oben auf das Protokoll der Punkt-zu-Punkt Ebene 2 (PPPoE).

17. Die Zugangssteuereinheit nach Anspruch 16, ferner umfassend Mittel zum Anfragen einer IP Adresse von einem Server für ein Protokoll einer dynamischen Host-Konfiguration, nachdem ein Benutzer durch sein öffentliches Landmobilfunknetz erfolgreich authentifiziert worden ist.

18. Eine Zugangssteuereinheit nach Anspruch 17, ausgebildet zum Kommunizieren mit einem drahtlosen Endgerät über einen Zugangspunkt.

19. Eine Zugangssteuereinheit nach Anspruch 17, ausgebildet zum Kommunizieren mit einem öffentlichen Landmobilfunknetz über einen Authentifizierungs-Gateway.

20. Eine Zugangssteuereinheit nach Anspruch 17, ausgebildet zum Kommunizieren über einen zum Authentifizieren von lokalen Benutzern eines öffentlichen lokalen Netzes verantwortlichen Authentifizierungsserver mit einem Authentifizierungs-Gateway.

21. Eine Zugangssteuereinheit nach einem der Ansprüche 15 bis 20, wobei das auf der Anwendungsebene angeordnete Authentifizierungsprotokoll ein erweiterbares Authentifizierungsprotokoll ist.

22. Die Zugangssteuereinheit nach Anspruch 21, wobei dieses erweiterbare Authentifizierungsprotokoll über ein RADIUS-Protokoll transportiert wird.

23. Die Zugangssteuereinheit nach Anspruch 21, wobei dieses erweiterbare Authentifizierungsprotokoll über ein Durchmesser-Protokoll (Englisch: Diameter Protocol) transportiert wird.

24. Ein drahtloses Endgerät mit einer SIM Karte, die zum Ausführen einer SIM-basierten Authentifizierungsprozedur zugänglich ist, wobei das drahtlose Endgerät eine Funktionalität zum Agieren als ein Client eines Protokolls einer Punkt-zu-Punkt Ebene 2 (PPPoE) umfasst und das oben auf diesem Protokoll der Punkt-zu-Punkt Ebene 2 ein erweiterbares Authentifizierungsprotokoll aufweist, wobei das drahtlose Endgerät gekennzeichnet ist durch Empfangen einer IP Adresse, nachdem eine erfolgreiche SIM-basierte Authentifizierungsprozedur ausgeführt worden ist, wobei die IP Adresse benutzbar ist, um eine IP Verbindungsfähigkeit zu erhalten.

25. Ein Telekommunikationssystem umfassend ein drahtloses lokales Netz mit mindestens einem Zugangspunkt, einem öffentlichen Landmobilfunknetz und mindestens einer mit einer SIM Karte ausgestatteten und zum Lesen von deren Teilnehmerdaten ausgebildeten Endgerätapparatur, dadurch gekennzeichnet, dass es ferner die Zugangssteuereinheit nach den Ansprüchen 15 bis 23 umfasst, um Benutzern des drahtlosen mobilen Netzes, die Teilnehmer des öffentlichen Landmobilfunknetzes sind, eine SIM-basierte Teilnehmerauthentifizierung zu erlauben.

Es folgen 4 Blatt Zeichnungen

Anhängende Zeichnungen

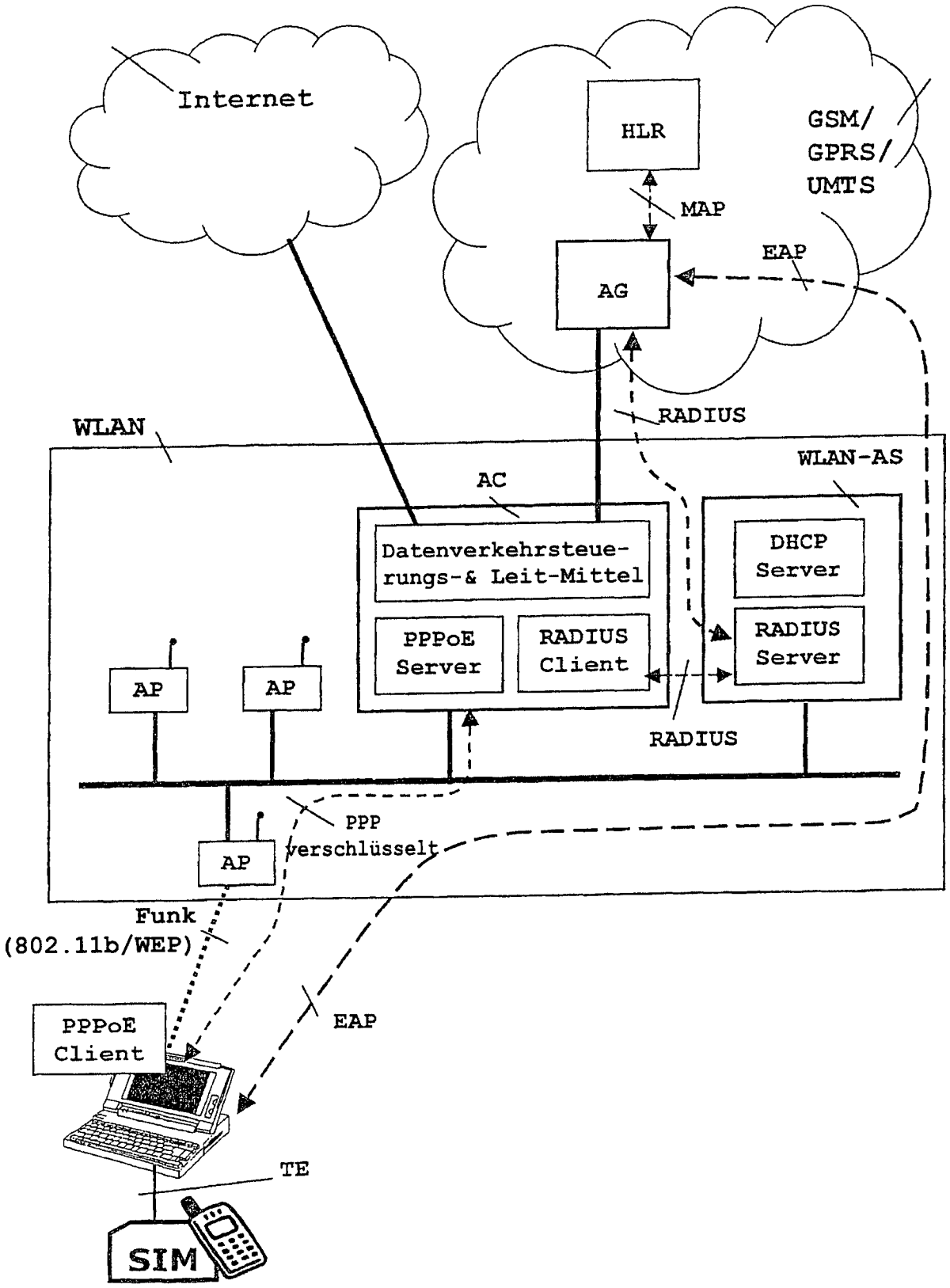

FIG.-1-

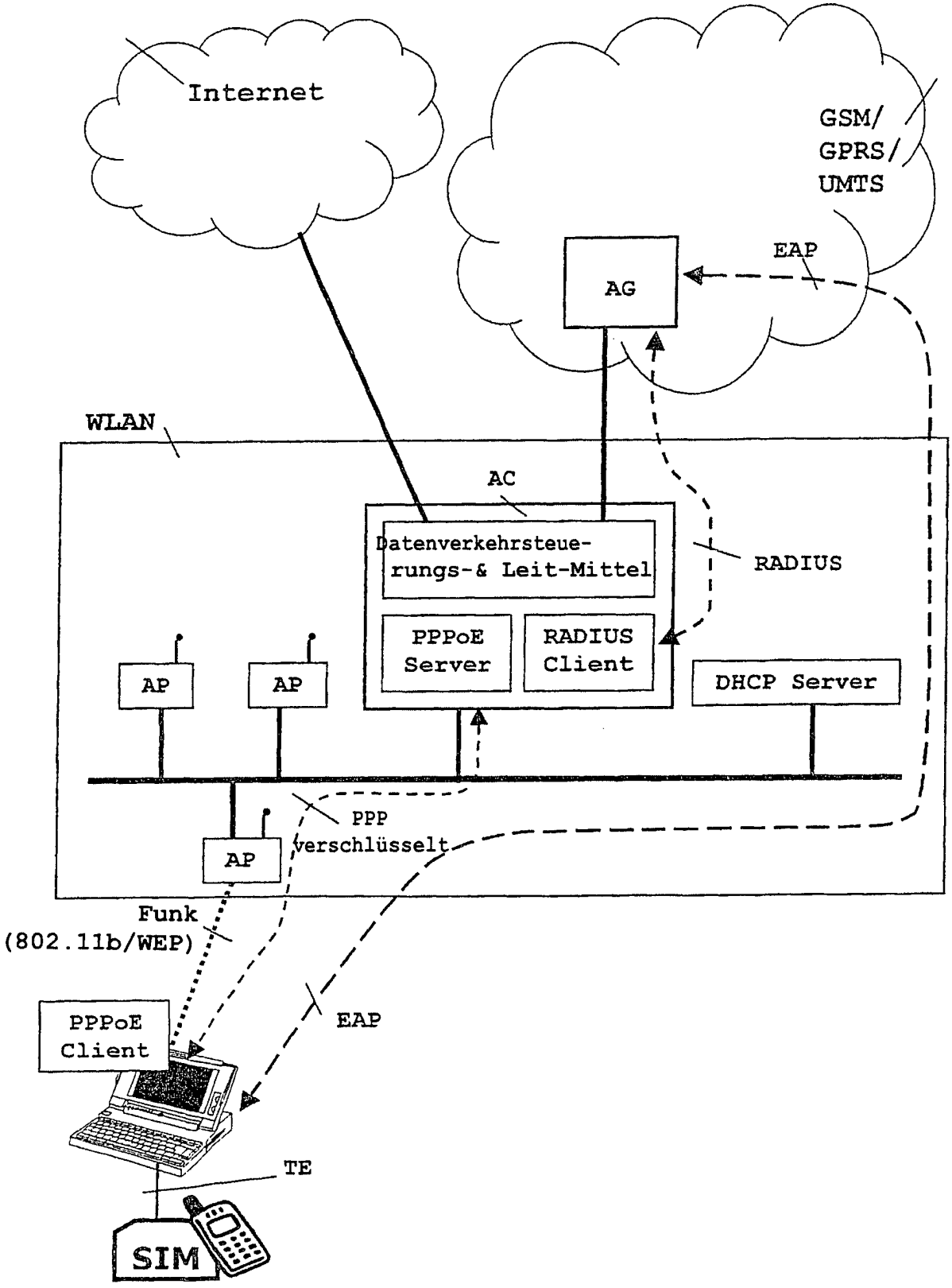
Internet
GSM/
GPRS/
UMTS
AG
EAP
WLAN
AC
Datenverkehrsteue-
rungs-& Leit-Mittel
RADIUS
PPPoE
Server
RADIUS
Client
DHCP Server
AP
AP
AP
PPP
verschlüsselt
Funk
(802.11b/WEP)
PPPoE
Client
EAP
TE
SIM

FIG.-2-

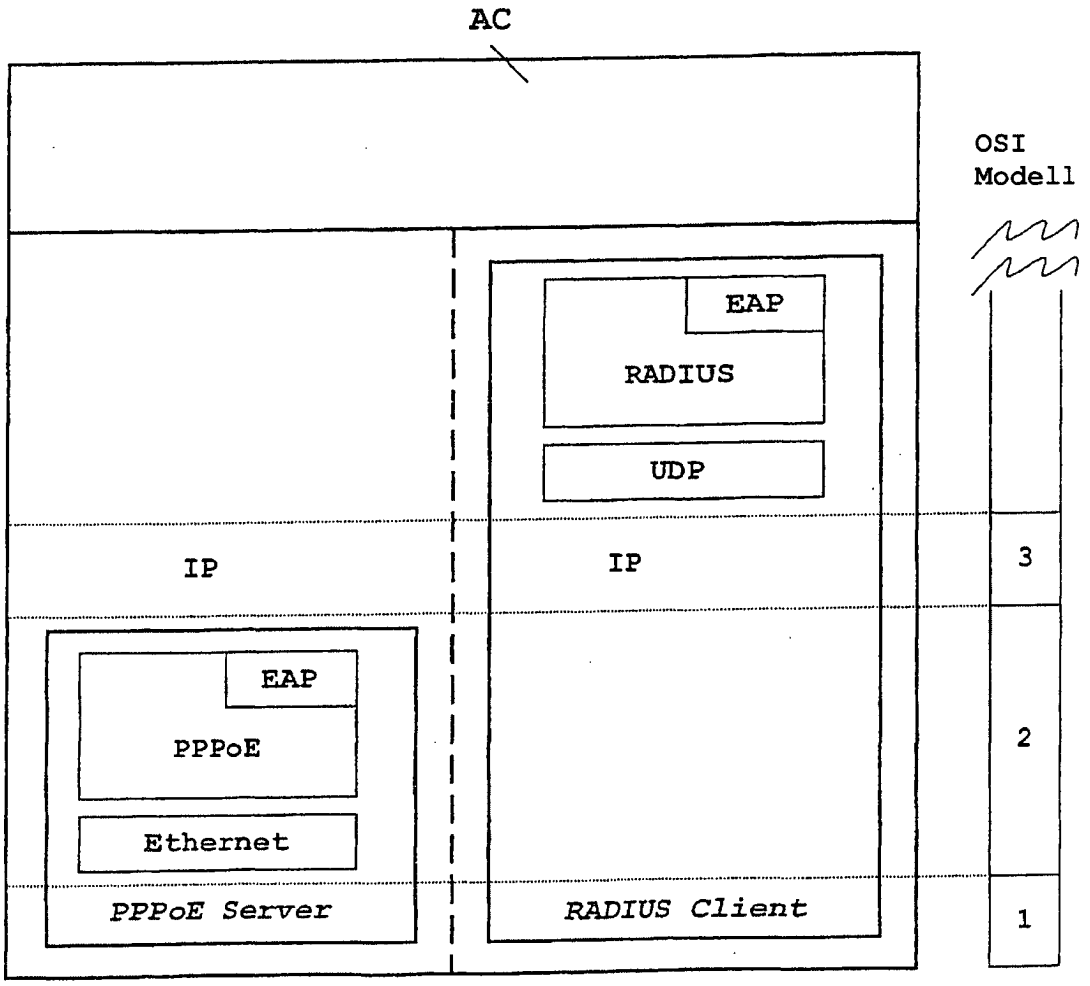
AC
OSI
Modell
EAP
RADIUS
UDP
IP
IP
3
EAP
PPPoE
Ethernet
2
PPPoE Server
RADIUS Client
1

FIG.-3-

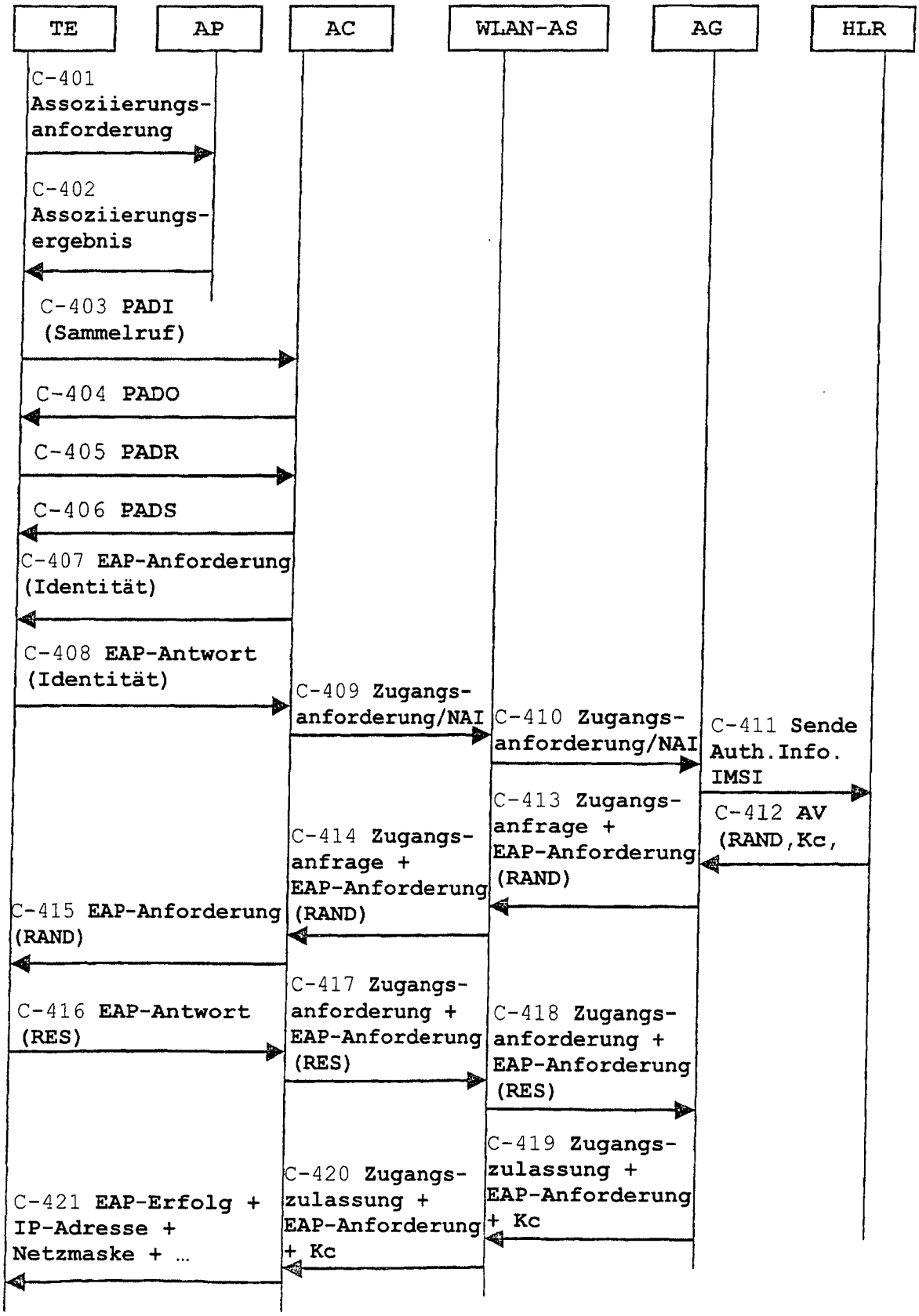
TE
AP
AC
WLAN-AS
AG
HLR
C-401 Assoziierungs-anforderung
C-402 Assoziierungs-ergebnis
C-403 PADI (Sammelruf)
C-404 PADO
C-405 PADR
C-406 PADS
C-407 EAP-Anforderung (Identität)
C-408 EAP-Antwort (Identität)
C-409 Zugangs-anforderung/NAI
C-410 Zugangs-anforderung/NAI
C-411 Sende Auth.Info. IMSI
C-412 AV (RAND,Kc,
C-413 Zugangs-anfrage + EAP-Anforderung (RAND)
C-414 Zugangs-anfrage + EAP-Anforderung (RAND)
C-415 EAP-Anforderung (RAND)
C-416 EAP-Antwort (RES)
C-417 Zugangs-anforderung + EAP-Anforderung (RES)
C-418 Zugangs-anforderung + EAP-Anforderung (RES)
C-419 Zugangs-zulassung + EAP-Anforderung + Kc
C-420 Zugangs-zulassung + EAP-Anforderung + Kc
C-421 EAP-Erfolg + IP-Adresse + Netzmaske + ...

FIG.-4-