WissenHeute Jg. 57 7/2004

# Integration von WLAN mit GPRS- und UMTS-Netzen.

Für Mobilfunkbetreiber ist WLAN (Wireless Local Area Network) neben UMTS (Universal Telecommunications System) und GSM/GPRS (Global System for Mobile Communications/General Packet Radio Service) ein wichtiger Baustein für das Multimedia-Angebot der Zukunft. Von entscheidender Bedeutung ist daher die Frage der Integration von WLAN-Hotspots in die vorhandene Mobilfunkinfrastruktur. Die Standardisierungsorganisation 3GPP (Third Generation Partnership Project[1]) arbeitet daher an einer Architektur, die verschiedene Integrationsszenarien von WLAN und zellularem Mobilfunk erlaubt. Diese Architektur wird in 3GPP TS 23.234 [1] spezifiziert und wird nachfolgend vorgestellt. Ein endgültiger Standard ist noch nicht verabschiedet, wenngleich die Anforderungen sowie die grundlegenden Verfahren bereits festliegen und ein Abschluss kurz bevor steht.

**Der Autor**

Dipl.-Ing. Stefanus Römer ist seit 1994 bei der Deutschen Telekom im Produktmanagement tätig und hat bereits mehrere Beiträge zum Thema „Mobile Datenkommunikation“ in den Unterrichtsblättern und WissenHeute veröffentlicht. Seit 2001 arbeitet er als Produktmanager bei T-Mobile, wo er insbesondere für das Produkt Mobile IP VPN und für mobile Intranet-Access-Lösungen zuständig ist.

## Einleitung

Auf Grund einer nahezu flächendeckenden Netzverfügbarkeit und weltweiter Roaming-Möglichkeiten[2] ermöglicht GSM/GPRS (2,5 G) und/oder UMTS-Netze (3 G) eine hohe Mobilität. Für den Kunden bedeutet dies, dass er fast überall auf 2,5-G- oder 3-G-Dienste zugreifen kann und dass aktive Anwendungen und/oder Dienste selbst bei einem Zellwechsel nicht unterbrochen werden. Diese letzte Eigenschaft bezeichnet man als „Service Continuity“. So ist es zum Beispiel für jeden Mobilfunkkunden heute selbstverständlich, dass er bei einer Fahrt auf der Autobahn auch mit hoher Geschwindigkeit unterbrechungsfrei telefonieren kann oder dass ein Spediteur seine Lkw-Flotte jederzeit über GPRS oder

[1] Das 3GPP ist eine gemeinsame Initiative europäischer, US-Amerikanischer, japanischer und koreanischer Standardisierungsorganisationen, die für die Spezifikation und Standardisierung von UMTS zuständig ist.

[2] Siehe hierzu den Beitrag „GPRS Roaming in GSM-Netzen“, Unterrichtsblätter Nr. 8/2003, S. 456 ff.

**Das Thema im Überblick**

Das Hauptmerkmal der Wireless-LAN-Technik (WLAN) besteht in der Bereitstellung eines drahtlosen Zugangs zu einem Lokalen Netz (Local Area Network = LAN). Experten gehen davon aus, dass die Nutzung dieser Zugangstechnik im privaten und öffentlichen Bereich sowie insbesondere die Verbreitung von öffentlichen Internet-Zugangspunkten in so genannten Hotspots, wie beispielsweise Flughäfen, Bahnhöfen oder Hotels, stark zunehmen wird. Laut aktuellen Studien gibt es weltweit bereits über 40 000 Hotspots. Schon heute wird WLAN in vielen privaten Haushalten und Unternehmen als schnurloser Zugang zum DSL-(Digital Subscriber Line-)Anschluss und/oder zum lokalen Netz genutzt und nimmt somit im Bereich der Datenkommunikation neben DSL eine zentrale Rolle ein. Gerade Mobilfunkanbieter (z. B. T-Mobile) sehen in dieser mobilen Zugangstechnik eine wichtige Ergänzung ihres Angebot-Portfolios.

mittels SMS (Short Message Service) disponiert, während diese unterwegs ist. Zellulare Mobilfunksysteme zeichnen sich zudem durch ein hohes Sicherheitsniveau in Bezug auf Authentizität[3] und Übertragungssicherheit aus.

Im Vergleich zu den Übertragungstechniken WLAN (z. B. IEEE 802.11b [Institute of Electrical and Electronics Engineers Inc.] mit in der Praxis bis zu 6 Mbit/s) oder DSL (z. B. ADSL [Asymmetric Digital Subscriber Line] mit bis zu 1,5 Mbit/s) sind die erzielbaren Übertragungsraten in zellularen Mobilfunknetzen erheblich geringer. Manche Anwendungen und Protokolle, die für eine reine LAN-(Local Area Network-) oder Festnetzumgebung entwickelt wurden, sind beispielsweise über GPRS ohne besondere Anpassungen nicht nutzbar[4].

Demgegenüber erlauben WLAN-Netze sehr viel höhere Datenraten von mehreren Megabit pro Sekunde, bieten jedoch bislang eine unzureichende Sicherheit für unternehmenskritische Anwendungen und sind räumlich sehr begrenzt. Die Übertragungstechnik WLAN wurde ursprünglich als schnurlose Erweiterung vorhandener Lokaler Netze ausschließlich für den unternehmensinternen Einsatz entwickelt. Die notwendige Daten- und Zugangssicherheit gewährleistet bereits eine entsprechend sichere Umgebung mit Hilfe von Personenkontrolle und/oder Gebäudesicherheit.

Erst seit kurzem wird diese Technik auch von Mobilfunkanbietern in stark frequentierten Orten wie Flughäfen, Bahnhöfen oder Hotels (Hotspots) eingesetzt, um einen öffentlichen Zugang zum Internet anzubieten. Da Hotspots jedoch öffentlich für jeden zugänglich sind, ist ein auf physischer Personenkontrolle und Gebäudesicherheit beruhendes Sicherheitskonzept wie im Bereich der internen Unternehmensnetze nicht umsetzbar. Das Sicherheitsprotokoll WEP (Wired Equivalent Privacy[5]), das im WLAN-Standard vorgesehen ist, kann zudem mit frei verfügbarer Software sehr leicht umgangen werden, weil es schwerwiegende Sicherheitslücken insbesondere im Bezug auf das Schlüsselmanagement aufweist.

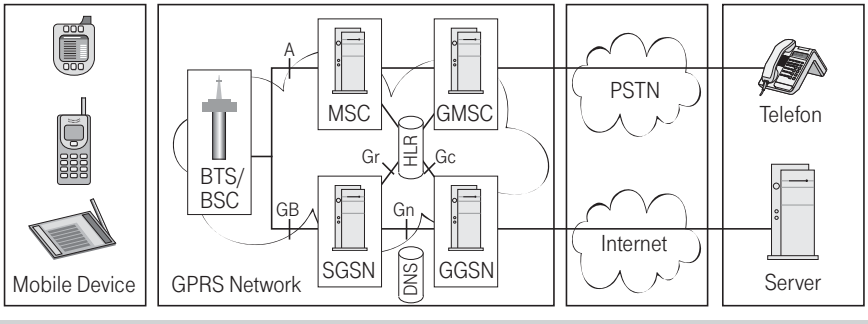
Durch eine Integration von öffentlichen WLAN-Hotspots mit 2,5-G- und 3-G-Netzen

[3] **Authentizität:** Echtheit, Glaubwürdigkeit.

[4] Siehe hierzu die Beiträge „Mit GPRS ins Intranet – Optimierungsmaßnahmen für den praktischen Einsatz in Unternehmensnetzen", Unterrichtsblätter Nr. 11/2001, S. 626 und „Mit GPRS ins Intranet – Outlook-Optimierung mit Mobile Office Optimizer", Unterrichtsblätter Nr. 11/2002, S. 580 ff.

[5] Siehe hierzu den Beitrag „Datensicherheit in Bluetooth- und Wireless-Lan-Funknetzen", Unterrichtsblätter Nr. 7/2002, S. 332 ff.

**Bild 1** Erweiterte Netzarchitektur von GSM durch GPRS




| | | | |
|---|---|---|---|
| A... Gx | Schnittstellenbezeichnung | GMSC | Gateway MSC |
| BSC | Base Station Controller | GPRS | General Packet Radio Service |
| BTS | Base Transceiver Station | HLR | Home Location Register |
| DNS | Domain Name System/Server | PSTN | Public Switched Telephone Network |
| GGSN | Gateway GPRS Support Node | SGSN | Serving GPRS Support Node |

lassen sich die genannten Vorzüge beider Techniken kombinieren. Ein besonderer Vorteil für die Betreiber von zellularen Mobilfunknetzen (z. B. T-Mobile) ist die Nutzung der vorhandenen Kundenbasis für die Vermarktung von WLAN.

Die nachfolgenden Ausführungen vermitteln zunächst die wichtigsten Grundlagen des zellularen Mobilfunks (2,5 G, 3 G) und WLAN, die für das Verständnis einer Integrationsarchitektur notwendig sind, bevor abschließend die verschiedenen Ansätze zur Integration beider Techniken beschrieben werden.

## Grundlagen 2,5-G-/3-G-Systemarchitektur

Das GPRS[6] erweitert die bestehende GSM-Netzarchitektur um zwei neue logische Paketvermittlungsknoten, den Serving GPRS Support Node (SGSN) und den Gateway GPRS Support Node (GGSN) (Bild 1). Diese werden auch für UMTS (3 G) unverändert genutzt. Der funktechnische Teil der GSM-Architektur, bestehend aus den Basisstationen (Base Transceiver Station = BTS) und den Steuereinheiten (Base Station Controller = BSC), wird für GPRS weiterhin genutzt. Bei UMTS wird dieser funktechnische Teil durch eine neue Zugangstechnik ersetzt. Die nachfolgenden Ausführungen gelten gleichermaßen für GPRS wie für UMTS.

Der SGSN ist über das so genannte Gb-Interface mit dem funktechnischen Teil des GSM- bzw. UMTS-Netzes verbunden. Er besitzt einen SS7-Anschluss (Signaling System No. 7 = Zeichengabesystem Nr. 7) für die Kommunikation mit der zentralen Teilnehmerdatenbank des GSM- und/oder UMTS-Netzes, dem Home Location Register (HLR), bzw. mit der mobilen Vermittlungsstelle für die leitungsvermittelten Dienste, dem Mobile Switching Center (MSC). Darüber hinaus ist ein IP-(Internet Protocol-)Anschluss für die Kommunikation mit den anderen GPRS Support Nodes vorhanden. Die Aufgaben dieses Knotens entsprechen größtenteils den Funktionen der MSC, wie beispielsweise Authentifizieren der Mobilstationen und Durchführen des Mobility Management[7]. Er besitzt eine integrierte Datenbasis, in der das Teilnehmerprofil und Mobility-Management-Informationen über die eingebuchten Mobilstationen temporär gespeichert werden.

Eine weitere Aufgabe dieses Knotens besteht in der Verschlüsselung der übertragenen Daten und der Erfassung von Abrechnungsdaten. Der GGSN bildet die interne GSM-Adresse (International Mobile Subscriber Identity = IMSI[8]) auf eine IP-Adresse ab. Diese IP-Adresse kann fest oder temporär einer IMSI zugeordnet werden, und zwar entweder durch den internen RADIUS[9] im GGSN selber oder durch einen externen RADIUS- oder einen DHCP-(Dynamic Host Configuration Protocol-)Server. Meldet sich eine Mobilstation (MS) für den GPRS-Dienst an, wird dementsprechend eine temporäre oder fest der IMSI zugeordnete IP-Adresse aktiviert. Nach der Aktivierung können ankommende Datenpakete der Mobilstation über den SGSN, dem BSC und der BTS zugestellt und empfangen werden.

Von zentraler Bedeutung für die Funktionsweise eines GPRS-Netzes ist der Domain Name Service (DNS). Die Aufgabe eines DNS ist es allgemein, einen Domain-Name in eine IP-Adresse zu übersetzen. Zur Adressierung externer IP-Netze (z. B. Internet, Informationsportale oder Unternehmensnetze) wird innerhalb des GPRS-Netzes jeweils ein Access Point Name (APN) verwendet.

Der APN ist – vereinfacht ausgedrückt – ein Domain-Name eines externen IP-Netzes nach RFC 1035 (Request For Comments[10]). Er hat eine Länge von bis zu 63 alphanumerischen Zeichen und wird nur innerhalb des GPRS-Backbone benutzt. Er dient zum einen dem SGSN zur Auswahl des richtigen GGSN und zum anderen dem GGSN zur Auswahl des richtigen externen Zielnetzes. Die Auflösung

---

6 Siehe hierzu den Beitrag „Mit GPRS ins Intranet – Das Produkt LAN to LAN GPRS Access“, Unterrichtsblätter Nr. 3/2001, S. 168 ff.

7 Das **Mobility Management** ist ein Verfahren in zellularen Mobilfunksystemen, mit dem in den zentralen Netzelementen MSC und/oder SGSN die Information über den aktuellen Aufenthaltsbereich (Local Area) einer Endstelle aktualisiert wird. Diese Gebietsinformation muss stets aktuell sein, um kommende Verbindungswünsche bearbeiten zu können.

8 **IMSI:** Abk. International Mobile Subscriber Identity, dt. Internationale Mobilfunk-Teilnehmerkennung. Im terrestrischen Mobilfunksystem GSM die internationale, höchstens fünfzehnstellige Kennung des GSM-Teilnehmers, die auf der Chipkarte (Subscriber Identity Module = SIM) des Mobilfunkteilnehmers gespeichert ist und dem Teilnehmer nicht bekannt ist. Der Zusammenhang zwischen der Kennung IMSI und der GSM-Rufnummer (Mobile Station ISDN Number = MSISDN) ist nur dem Netz (Home Location Register) bekannt. Hat der Teilnehmer mehrere GSM-Dienste (z. B. Telefon-, Telefax- und Datendienst) über eine Chipkarte (SIM) abonniert, so erhält er für jeden Dienst eine eigene MSISDN.

9 **RADIUS:** Abk. Remote Authentication Dial-in User Service. Für Remote-Access-Anwendungen entwickeltes Sicherheitsprotokoll (RFC 2138, 2139), um unerlaubte externe Zugriffe auf Daten und Systeme zu verhindern. RADIUS funktioniert nach dem Client-Server-Konzept und legt die Kooperation zwischen einem AAA-Server (Authentication, Authorization and Accounting Server) und einem Network Access Server (NAS) fest. In diesem Konzept kann der AAA-Server als RADIUS-Server angesehen werden, in dem sämtliche Informationen über Remote-Benutzer zur Verfügung stehen. Der RADIUS-Client stellt ein Funktionsmodul dar, das auf dem NAS installiert wird.

10 **Request for Comments:** Sammlung von Empfehlungen, Artikeln und Standards (RFC-Standards), in denen netzrelevante Konventionen und allgemeine Informationen zum Internet festgehalten sind. Als RFC sind auch die Anregungen und Verbesserungsvorschläge bezeichnet, die die Teilnehmer des Internets beim so genannten RFC-Editor einreichen.

**Verwendete Abkürzungen**

| | |
|---|---|
| 2,5 G | Weiterentwicklung von Mobilfunknetzen der zweiten Generation (z. B. GPRS innerhalb von GSM) |
| 3 G | Mobilfunknetze der dritten Generation (z. B. UMTS) |
| 3GPP | Third Generation Partnership Project |
| AAA | Authentication, Authorization and Accounting Server |
| AD | Access Device |
| ADSL | Asymmetric Digital Subscriber Line |
| AKA | Authentication and Key Agreement |
| AP | Access Point |
| APN | Access Point Name |
| AR | Access Router |
| BSC | Base Station Controller |
| BTC | Base Transceiver Station |
| CHAP | Challenge Handshake Authentication |
| CS | Cable Switching (Leitungsvermittlung) |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name System/Server |
| DSL | Digital Subscriber Line |
| EAP | Extensible Authentication Protocol |
| GGSN | GPRS Gateway Support Node |
| GPRS | General Packet Radio Service |
| GSM | Global System for Mobile Communications |
| HA | Home Agent |
| HLR | Home Location Register |
| IEEE | Institute of Electrical and Electronics Engineers Inc. |
| IMSI | International Mobile Subscriber Identity |
| IP | Internet Protocol |
| ISP | Internet Service Provider |
| ITU | International Telecommunication Union |
| IV | hier: Initialisation Vector |
| LAN | Local Area Network |
| MAP | Mobile Application Part |
| MN | Mobile Node |
| MSC | Mobile Switching Center |
| MSISDN | Mobile Station ISDN Number |
| NAI | Network Access Identifier |
| NAPT | Network Address and Port Translation |
| NAS | Network Access Server |
| OSI | Open System Interconnection |
| PAP | Password Authentication Protocol |
| PDG | Packet Data Gateway |
| PDP | Packet Data Protocol |
| PPP | Point to Point Protocol |
| PS | Packet Switching |
| QoS | Quality of Service |
| RADIUS | Remote Authentication Dial-in User Service |
| RFC | Request for Comments |
| SGSN | Service Gateway Support Node |
| SIM | Subscriber Identity Module |
| SMS | Short Message Service |
| SS7 | Signaling System No. 7 |
| SSG | Service Selection Gateway |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| UMTS | Universal Mobile Telecommunications System |
| USIM | Universal Subscriber Identification Module |
| VLR | Visitor Location Register |
| VPN | Virtual Private Network |
| WAG | WLAN Access Gateway |
| W-APN | WLAN-Acces Point Name |
| WEP | Wireless Equivalency Privacy |
| WLAN | Wireless Local Area Network |
| WPA | Wi-Fi Protected Access |

des APN in die IP-Adresse des GGSN wird durch eine Anfrage des SGSN am Domain Name Server vorgenommen. Vor dem Senden von IP-Datenpaketen muss die Mobilstation eine GPRS-Einbuchung (GPRS Attach) und eine so genannte PDP[11]-Kontext-Aktivierung (PDP Context Activation) durchführen.

Die GPRS-Einbuchung setzt das Netz darüber in Kenntnis, dass die MS im Netz vorhanden ist. Die Einbuchung wird durch die MS beim SGSN vorgenommen. Bei der GPRS-Einbuchung gibt die Mobilstation ihre Identität bekannt (IMSI oder Packet TMSI[12]) und gibt an, ob die Einbuchung für Paketvermittlung (PS Attach) oder die kombinierte Einbuchung für Paketvermittlung und Leitungsvermittlung/IMSI (PS und CS/IMSI Attach) angefordert wird.

Zum Senden und Empfangen von GPRS-Daten führt die Mobil Station nach der GPRS-Einbuchung eine PDP-Kontext-Aktivierung aus. Die PDP-Kontext-Aktivierung macht die MS dem betreffenden GGSN bekannt, woraufhin Datenübertragungen über den GGSN in externe IP-Netze möglich sind. Die Adressierung des externen Zielnetzes wird von der Mobil Station im Rahmen der Kontext-Aktivierung unter Angabe des APN vorgenommen. Sofern die MS keinen APN angibt, wird die Verbindung mit Hilfe eines „Default-APN" aufgebaut, der im SGSN fest hinterlegt ist. In der Regel verbirgt sich hinter diesem Default-APN das Internet.

Der GGSN wendet bei jeder Anforderung einer PDP-Kontext-Aktivierung eine Zugangskontrollfunktion (Admission Control) an. Diese Funktion zieht die weitere Bearbeitung der Anforderung, die Verhandlung der QoS (Quality of Service) mit der Mobil Station oder deren Zurückweisung nach sich. Das System prüft auch, ob der beauftragte Dienst (Subscription) die Berechtigung für den Zugriff auf ein bestimmtes externes Netz eines ISP (Internet Service Provider) oder eines Unternehmens einschließt.

## Grundlagen eines WLAN

Das Standardisierungs-Komitee IEEE 802, das weltweit für die Standardisierung von LAN-Technologien zuständig ist, hat bereits 1997 in der Serie IEEE 802.11 den ersten Standard für WLAN festgelegt, der in der Folge durch verschiedene Ergänzungen vervollständigt wurde. Seit der Veröffentlichung des Substandards IEEE 802.11b im Jahr 1999

[11] **PDP:** Abk.: Packet Data Protocol; allgemeiner Begriff für ein Protokoll, das Daten in diskreten Einheiten bzw. Paketen überträgt. Beispiele: IPv4 oder X.25. GPRS von T-Mobile unterstützt derzeit den PDP-Typ IPv4.

[12] **TMSI:** Abk. Temporary Mobile Subscriber Identity, dt. Temporäre Teilnehmerkennung. Im GSM-System die von der Besucherdatei Visitor Location Register (VLR) für die einzelne Mobilfunkverbindung vergebene Kennung mit Funktionen im Rahmen der GSM-Sicherheitsmechanismen.

**Tabelle** **Standards nach IEEE 802.11 (Übertragungstechnik und -methoden)**

| IEEE-Standard | Beschreibung |
|---|---|
| 802.11 | Erster WLAN-Standard mit einer Übertragungsrate von 1 Mbit/s bzw. 2 Mbit/s mit Infrarot-Technik. |
| 802.11a | Ergänzung zum Basis-Standard: 5-GHz-Band mit Kanalbandbreite von 22 MHz; entfernungsabhängige Datenraten: 6 Mbit/s bis 54 Mbit/s; **Reichweiten:** etwa 30 m (innerhalb von Gebäuden) etwa 60 m (außerhalb von Gebäuden). |
| 802.11b | Ergänzung zum Basis-Standard: 2,4-GHz-Band mit Kanalbandbreite von 22 MHz; Datenraten: von 1 Mbit/s bis 11 Mbit/s; **Reichweiten:** etwa 50 m (innerhalb von Gebäuden) etwa 100 m (außerhalb von Gebäuden). |
| 802.11c | Ergänzungen, um Verfahren zur Verbindung zweier Netzwerke. |
| 802.11d | Harmonisierung bzw. Definition bestimmter WLAN-Parameter. |
| 802.11e | Erweiterung um Qualitätsklassen (QoS): WME (Wi-Fi Multimedia Extensions) und WSM (Wireless Scheduled Multimedia). |
| 802.11f | Inter Access Point Protocol für Roaming über mehrere WLAN-Zellen verschiedener Hersteller. Die APs werden über LAN-Bridges miteinander verbunden. |
| 802.11g | Erweiterung der maximalen Übertragungsbandbreite im 2,4-GHz-Band auf 54 Mbit/s. |
| 802.11h | Regionalanpassung für IEEE 802.11a für einige europäische Länder zur Harmonisierung mit HiperLAN/2: Ergänzung um Dynamic Frequency Selection (DFS) und Transmission Power Control (TPC). |
| 802.11i | Ergänzung um ein sicheres Authentisierungsverfahren für WLANs mit dynamischer Schlüsselzuweisung Industriestandard WPA II bekannt. Mit einer Veröffentlichung wird bis Ende 2004 gerechnet. |

war es zum ersten Mal möglich, über einen schnurlosen Zugang die gleichen Leistungsparameter (Performance-Werte) zu erzielen wie in einem leitungsgebundenen LAN. Der Substandard IEEE 802.11b hat sich seither zum defacto-Standard entwickelt und kommt in den meisten Implementierungen zum Einsatz.

Wie der Standard IEEE 802.3 (Ethernet) beschreiben die IEEE-802.11-Standards ausschließlich die beiden untersten Schichten des OSI-Referenzmodells (Open Systems Interconnection), nämlich den Physical Layer und den Data Link Layer. Das bedeutet, dass z. B. alle LAN-Anwendungen und Protokolle, insbesondere TCP/IP (Transmission Control Protocol/Internet Protocol[13]), uneingeschränkt über WLAN genutzt werden können. Der WLAN Access Point (AP) bzw. die Basisstation ist somit eine Layer 2 Bridge und verhält sich beispielsweise wie ein gewöhnlicher Ethernet-Hub. Die verschiedenen IEEE-802.11-Standards sind in der Tabelle aufgeführt.

Diese Standards nach IEEE 802.11 legen nicht nur das Übertragungsverfahren und die maximale Übertragungsgeschwindigkeit fest, sondern es werden auch Standards definiert, die bestimmte Dienstmerkmale, wie beispielsweise höhere Sicherheit, erlauben, eine Vereinheitlichung bestimmter Abläufe beinhalten oder Regionalanpassungen definieren, um bestimmte regulatorische Auflagen zu erfüllen. Viele dieser Methodenstandards sind noch nicht fertig spezifiziert. Wichtigster Vertreter dieser Methodenstandards ist IEEE 802.11i, der für WLAN eine neue Sicherheitsarchitektur mit verbesserten Authentifizierungs- und Verschlüsselungsmethoden festlegen soll. Obwohl dieser Standard noch nicht offiziell verabschiedet ist, gibt es bereits WLAN-Endgeräte, die diese Methode unterstützen[14]. (Eine abschließende Veröffentlichung dieses Substandards wird bis Ende 2004 erwartet.)

Eine Verbesserung der Sicherheitsarchitektur ist notwendig, weil das vorhandene Sicherheitsprotokoll WEP als unsicher eingestuft wird und z. B. mit frei verfügbaren Software-Tools (beispielsweise Airsnort, WepCrack) leicht zu umgehen ist. Außerdem bildet dieser neue Substandard IEEE 802.11i die Voraussetzung für eine Integration mit 2,5-G-/3-G-Mobilfunksystemen.

Die „Schwachstelle" von WEP ist insbesondere das Schlüsselmanagement. Die Schlüssel werden fest eingebracht und können nicht während der laufenden Nutzung geändert werden. In vielen Systemen wird ein einziger Schlüssel für alle Anwender genutzt. Zudem werden Steuerungsinformationen weder authentisiert noch verschlüsselt. Der eingebrachte Schlüssel ist entweder 40 Bit oder 104 Bit lang. Hieraus wird für die Verschlüsselung jedes einzelnen IP-Datenpakets jeweils ein neuer Schlüssel erzeugt, indem ein zufälliger Initialisierungswert, der Initialisation Vector (IV), von 24 Bit hinzugesetzt wird. Damit ergibt sich eine eigentliche Schlüssellänge von 64 Bit oder 128 Bit.

Damit das Datenpaket vom Empfänger entschlüsselt werden kann, wird dieser Initialisierungswert vor der Übertragung des jeweiligen Paketes im Klartext übertragen. Mit einer entsprechenden Software lässt sich in einem ausgelasteten WLAN-System durch Auswerten der Initialisierungswerte in der Regel nach wenigen Stunden der geheime Schlüssel extrahieren[15], so dass anschließend der Datenverkehr ungehindert mitgelesen werden kann.

Der IEEE-802.11i-Standard legt demgegenüber eine Rahmenarchitektur für eine verbesserte Sicherheit fest, in die sich wahlweise verschiedene Verfahren zur Authentisierung,

[13] Siehe hierzu den Beitrag „Die Protokoll-Familie TCP/IP", WissenHeute Nr. 3/2004, S.116 ff.

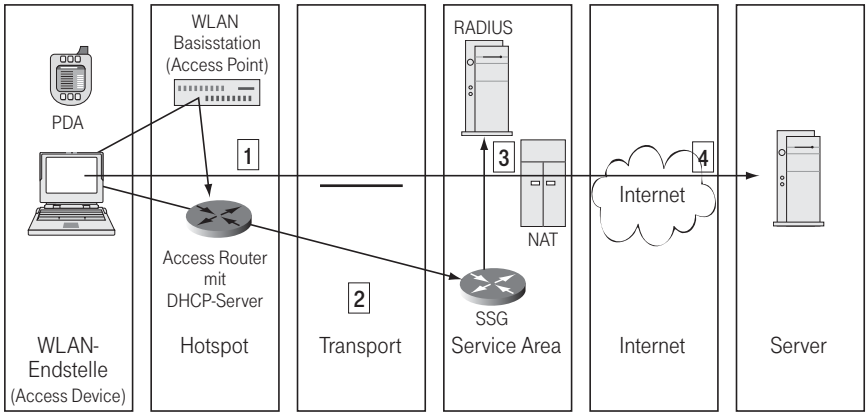
[14] Diese Endgeräte führen das Prädikat WPA-fähig (WPA steht für WiFi Protected Access, wobei WiFi für Wireless Fidelity steht und die amerikanische Bezeichnung für Funknetzwerke nach IEEE 802.11 ist.)

[15] **extrahieren:** herausziehen.

Schlüsselverwaltung und Verschlüsselung integrieren lassen. Somit können anerkannt zuverlässige Sicherheitsverfahren, wie beispielsweise aus dem Bereich der 2,5-G-/3-G-Mobilfunksysteme leicht integriert und somit unverändert auch für WLAN-Systeme genutzt werden. Dies wird möglich durch den Einsatz des Extensible Authentication Protocol (EAP, RFC2284).

Das EAP ist eine Erweiterung des Point to Point Protocol (PPP, RFC 1661), das z. B. für die Einwahl in IP-Netze zur Anwendung kommt. Mit Hilfe von EAP können somit bei der Einwahl über PPP unterschiedliche Authentisierungs- und Verschlüsselungsmethoden vereinbart werden. Bekannte Authentisierungsverfahren, die in diesem Zusammenhang eingesetzt werden, sind beispielsweise PAP (Password Authentication Protocol, RFC 1334) oder CHAP (Challenge Handshake Authentication, RFC 1994). Weitere Verfahren, die im Rahmen einer Integration von WLAN mit 2,5-G-/3-G-Systemen wichtig werden, sind EAP SIM für GSM/GPRS (2,5 G) sowie EAP AKA[16] für UMTS (3 G).

**Bild 2** **WLAN-Architektur und Zugangsprozedur**




- Die WLAN-Endstelle wird aktiviert und erhält vom DHCP-Server des Access Router automatisch eine IP-Adresse.
- Der Benutzer startet den Browser und erhält über das SSG in der zentralen Service Area des Diensteanbieters automatisch eine Startseite mit Anmeldung.
- Benutzername und Kennwort werden von RADIUS überprüft.
- Nach erfolgter Anmeldung kann der Benutzer ungehindert auf beliebige Server im Internet zugreifen. Seine IP-Adresse wird dabei mit Hilfe von NAT auf eine öffentliche IP-Adresse abgebildet.

| | | | |
|---|---|---|---|
| DHCP | Dynamic Host Configuration Protocol | PDA | Personal Digital Assistant |
| IP | Internet Protocol | SSG | Service Selection Gateway |
| NAT | Network Adress Translation | | |

## WLAN-Netzwerkarchitektur und Zugangsprozedur

Obwohl es keinen allgemeinen Standard oder einen RFC für den Aufbau von WLAN-Zugangsnetzen gibt, hat sich dennoch eine bestimmte Architektur herausgebildet, die grundsätzlich von allen Systemen eingehalten wird. Der grundlegende Aufbau wird in Bild 2 gezeigt. Demnach besteht ein WLAN-Zugangssystem aus folgenden Komponenten:

- **Access Device (AD)**
  Das AD ist das WLAN-Endgerät des Benutzers. Vielfach besteht es aus einem Laptop mit einer WLAN-Einschubkarte. Diese verhält sich wie eine gewöhnliche Ethernet-Karte und wird genauso angesteuert. Um Zugang zu einem WLAN-Hotspot zu erhalten, startet der Benutzer lediglich seinen Browser. Danach wird ihm automatisch eine Startseite des jeweiligen WLAN-Diensteanbieters angezeigt, die so genannte „landing page". Auf dieser Seite muss er sich mit Benutzername und Kennwort authentisieren, bevor er in gewohnter Weise im Internet surfen oder beliebige andere Anwendungen (z. B. VPN-Clients[17] oder Netmeeting[18]) nutzen kann.
- **Access Point (AP) oder Basisstation**
  Sie verhält sich wie eine Layer 2 Bridge oder ein Ethernet Hub und bildet lediglich die beiden unteren Schichten des OSI-Modells ab. Diese Komponente stellt somit nur den physikalischen Zugang dar, enthält jedoch keine weitere Intelligenz.
- **Access Router (AR)**
  Der Router realisiert die Schicht 3 des OSI-Modells und ist zuständig für die Zuteilung einer IP-Adresse, die er in der Regel von einem DHCP-Server erfragt und anschließend dem jeweiligen Access Device zuordnet. Der DHCP-Server ist vielfach als Funktion Bestandteil des AR.
- **Service Selection Gateway (SSG)**
  Das SSG erlaubt in der Phase vor der Authentisierung, also unmittelbar nach dem Start, lediglich einen Zugriff mittels Browser. Alle anderen Protokolle und/oder Ports bleiben zunächst gesperrt, bis sich der Benutzer mit Benutzername und Kennwort authentisiert hat. Unabhängig davon welche Startseite der Benutzer gewählt hat, erhält dieser zunächst stets die Startseite des jeweiligen Hotspot-Betreibers, die landing page.
- **RADIUS mit den Benutzerkennungen und den jeweiligen Teilnehmerprofilen**
  Im RADIUS-System sind die einzelnen Benutzerdaten abgelegt, die zur Authentisierung benötigt werden. Hierzu übergibt das SSG jeweils mit Hilfe eines RADIUS Authentication Request den Benutzernamen und das Kennwort zur Prüfung an den RADIUS. Dieser antwortet entweder mit einem Accept oder einem Reject. Nach Ende der Session[19] oder nach Ab-

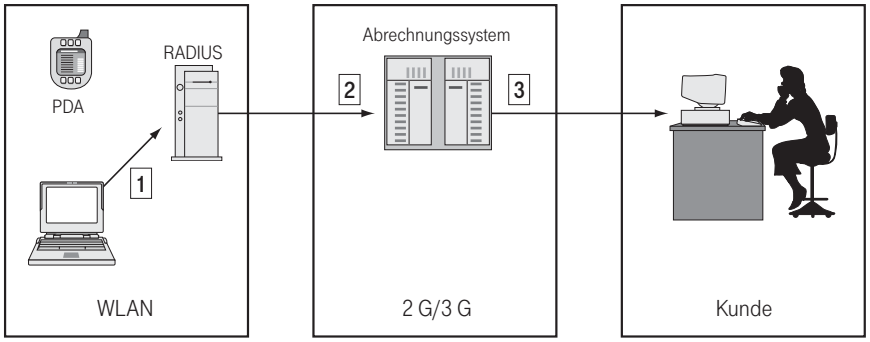
[16] Die Abkürzung AKA bedeutet hier Authentication and Key Agreement.

[17] **VPN-Clients:** Ein Software-Programm zum Aufbau einer VPN-(Virtual Private Network-)Verbindung zu einem VPN-Gateway. Ein VPN ermöglicht einen gesicherten Zugang und eine gesicherte Datenübertragung zu einem privaten Unternehmensnetz über öffentliche Datenplattformen, wie z. B. das Internet.

[18] **Netmeeting:** Anwendungs-Software, die eine direkte Kommunikation und einen Datenaustausch auf verschiedenen Ebenen (Ton, Bild, Text und Grafik) über die Internet-Technik ermöglicht.

[19] **Session (Sitzung):** allgemein der Zeitraum zwischen Starten und Beenden eines Programms, gelegentlich auch der Zeitraum zwischen Ein- und Ausschalten des Computers.

**Bild 3 Integrationsszenario 1 – Gemeinsame Abrechnung**




- Der Kunde authentisiert sich am WLAN-RADIUS mit seiner Benutzerkennung, die seine mobile Rufnummer (MSISDN) als Bestandteil enthält: z. B. 49171234567@t-mobile.de.
- Nach Ende der WLAN-Sitzung generiert der WLAN-RADIUS einen Abrechnungsdatensatz, der u. a. die Benutzerkennung enthält.
- Das Abrechnungssystem des 2-G-/3-G-Betreibers ermittelt aus dem Benutzernamen die mobile Rufnummer und ermittelt hierüber einen Rechnungsweg.

| | | | |
|---|---|---|---|
| MSISDN | Mobil Station ISDN Number | RADIUS | Remote Authentication Dial-in User Service |
| PDA | Personal Digital Assistant | WLAN | Wireless LAN |

lauf eines voreingestellten Zeitgebers übergibt das SSG dem RADIUS einen Abrechnungsdatensatz. Der RADIUS kann wiederum selbst als RADIUS-Proxy[20] arbeiten und alle Anfragen oder Nachrichten des SSG an einen fremden RADIUS weiterleiten. Die Auswahl des jeweiligen RADIUS wird dabei anhand des so genannten Network Access Identifiers (NAI) vorgenommen. Diese Eigenschaft ermöglicht ein Roaming der Teilnehmer in den Hotspots fremder Anbieter.

- **Network Address and Port Translation (NAPT)**
  Auf Grund der allgemeinen Knappheit an IP-Adressen werden innerhalb der WLAN-Hotspot-Umgebung in der Regel private IP-Adressen verwendet. Um dennoch eine Verbindung zum öffentlichen Internet zu ermöglichen, müssen diese privaten IP-Adressen immer einer öffentlichen IP-Adresse mittels NAPT zugeordnet werden.

## Einführung der Integrationsszenarien

Bei der Frage der Integration verschiedener technischer Systeme wie WLAN und zellularer Mobilfunk muss zunächst festgelegt werden, auf welcher Ebene eine Integration vorgenommen werden soll. Hier lassen sich folgende Integrationsstufen und -szenarien unterscheiden:

1. **Gemeinsame Abrechnung (common billing):** Auf dieser Integrationsebene werden die Abrechnungsdaten für genutzte WLAN-Dienste und 2,5-G-/3-G-Dienste auf einer gemeinsamen Rechnung zusammengeführt. Eine technische Integration ist damit jedoch nicht notwendigerweise verbunden.
2. **Gemeinsame Zugangskontrolle und Sicherheit (common access control and security):** Auf dieser Ebene werden für WLAN und 2,5-G-/3-G-Dienste die gleichen Zugangssysteme genutzt. Der Nutzer ist in beiden Zugangssystemen unter der gleichen einheitlichen Kennung bekannt. In der Regel umfasst diese Integrationsebene auch eine gemeinsame Abrechnung.
3. **Zugriff auf gemeinsame Dienste (access to common services):** Die Integration stellt über beide Zugangssysteme die gleichen Dienste bereit. Hierunter fallen beispielsweise Portaldienste oder Zugriff auf Unternehmensnetze; auch Roaming fällt unter dieses Szenario. Diese Integrationsstufe umfasst in der Regel sowohl eine gemeinsame Abrechnung als auch eine integrierte Zugangskontrolle.
4. **Service continuity mit Mobile IP:** Dieses Funktionsmerkmal ermöglicht den Wechsel zwischen WLAN und 2,5-G-/3-G-Dienste mit minimalem Datenverlust und kurzen Unterbrechungszeiten, jedoch ohne Sitzungsabbruch auf Dienste- oder Anwendungsebene. Beispielsweise kann hierdurch ein Benutzer mittels WLAN auf ein gemeinsames Informationsportal zugreifen. Während er den WLAN Hotspot verlässt, bucht sich sein Endgerät automatisch in ein UMTS-Netz ein, baut eine Verbindung auf und führt die Sitzung (Session) auf Anwendungsebene an der gleichen Stelle fort. Der Benutzer nimmt lediglich eine zeitliche Unterbrechung, jedoch keinen Abbruch war.

Je nach Integrationsgrad spricht man von „lose gekoppelten Systemen“ (loosely coupled systems), wenn nur eine Integration auf Abrechnungsebene realisiert ist. Bei „eng gekoppelten Systemen“ (tightly coupled systems) liegt eine volle Integration bis einschließlich Service continuity vor. Wireless-LAN kann dann neben UMTS und GPRS nur als eine weitere Funkschnittstelle (radio interface) betrachtet werden.

## Integrationsszenario 1: Gemeinsame Abrechnung

In diesem Szenario sind WLAN und 2,5-G-/3-G-Netze nur lose über ein gemeinsames Abrechnungssystem gekoppelt (Bild 3). Üblicherweise enthält der WLAN-Benutzername einen Bezug zur Teilnehmerkennung in 2,5-G-/3-G-Netzen anhand dessen eindeutig ein Abrechnungsweg identifiziert werden kann. Beim aktuellen WLAN-Angebot der T-Mobile besteht der WLAN-Benutzername im ersten Teil beispielsweise aus der mobilen Rufnummer (MSISDN) des jeweiligen T-Mobile Kunden und wird wie folgt gebildet:

<Benutzername> : = <MSISDN>@t-mobile. de

Dieser Benutzername wird als Kennung in die Abrechnungsdaten übernommen, die der

[20] **Proxy:** allgemein für Server, die einen „Stellvertreterdienst“ wahrnehmen; sie nehmen Anforderungen von einem Client entgegen und geben diese an das ursprüngliche Ziel weiter.

RADIUS-Server des WLAN-Zugangsnetzes erzeugt und an das gemeinsame Abrechnungssystem übermittelt.

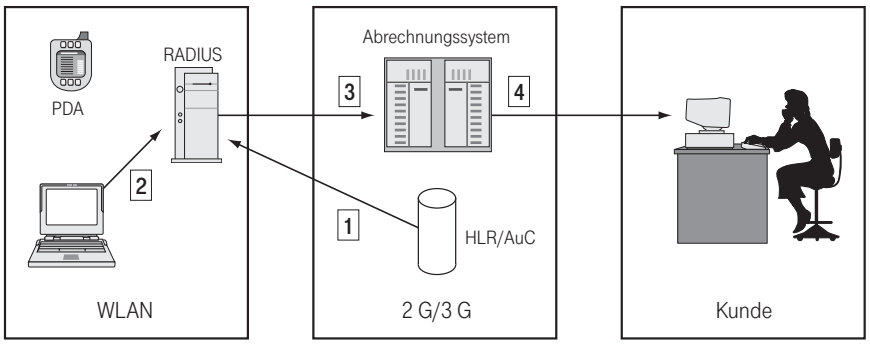
Der Teil „t-mobile.de“ des Benutzernamens wird als realm oder Network Access Identifier (NAI) bezeichnet und ist insbesondere für das Roaming-Verfahren von Bedeutung. In diesem Falle wird der RADIUS Authentication Request des SSG anhand des NAI vom RADIUS des „besuchten“ Netzes an den zuständigen RADIUS des Heimatnetzes, wo der jeweilige Benutzer bekannt ist, weitergeleitet. Der RADIUS des besuchten Netzes nimmt dabei die Funktion eines Proxy ein.

## Integrationsszenario 2: Gemeinsame Zugangskontrolle und Sicherheit

Die Grundlage für eine integrierte Zugangskontrolle und Sicherheit bildet der Substandard IEEE 802.11i, der sich noch in der Abstimmung befindet. Er legt eine Rahmenarchitektur für eine verbesserte Sicherheit fest, in die sich wahlweise verschiedene Verfahren zur Authentisierung, Schlüsselverwaltung und Verschlüsselung integrieren lassen. Der IEEE-802.11i-Standard sieht den Einsatz des Extensible Authentication Protocol (EAP, RFC 2284) vor. Hiermit können die vorhandenen Sicherheitsverfahren der 2,5-G- und/oder 3-G-Netze EAP SIM für GSM/GPRS (2,5 G) sowie EAP AKA für UMTS (3 G) unverändert auch für die WLAN-Zugangskontrolle genutzt werden (Bild 4). Hierzu sind selbstverständlich WLAN-Endgeräte mit einer SIM/USIM-Karte erforderlich, beispielsweise ein Laptop mit einem zusätzlichen Kartenleser.

Das EAP SIM ist ein Verfahren zur Authentisierung und zum Schlüsselmanagement, das auf dem gleichen Algorithmus beruht, wie er bei der Einbuchung einer SIM-Karte in ein GSM-Netz zur Anwendung kommt. Die Protokollnachrichten werden wie im Falle einer GSM-Einbuchung zwischen der SIM-Karte und einem Authentisierungs-Server ausgetauscht. Im Falle von GPRS/UMTS ist dieser Server der SGSN und im Fall von WLAN wird diese Funktion von einem RADIUS übernommen, der ebenfalls wie ein SGSN die Informationen zur Authentisierung und das Berechtigungsprofil über eine Standardschnittstelle (Mobile Application Part = MAP) ebenfalls vom HLR bezieht.

**Bild 4** **Integrationsszenario 2 – Gemeinsame Zugangskontrolle und Sicherheit**




- Der WLAN-RADIUS lädt vom HLR/AuC das Teilnehmerprofil herunter.
- Kunde authentisiert sich am WLAN-RADIUS mit seiner Benutzerkennung, die seine mobile Rufnummer (MSISDN) als Bestandteil enthält: z. B. 491711234567@t-mobile.de. Die Authentisierung wird mit Hilfe von EAP SIM für 2 G bzw. EAP AKA für 3 G vorgenommen.
- Nach Ende der WLAN-Sitzung generiert der WLAN-RADIUS einen Abrechnungsdatensatz, der die Benutzerkennung enthält.
- Das Abrechnungssystem des 2-G-/3-G-Betreibers ermittelt aus dem Benutzernamen die mobile Rufnummer und ermittelt damit einen Rechnungsweg.

| | | | |
|---|---|---|---|
| AKA | Authentication and Key Agreement | PDA | Personal Digital Assistant |
| AuC | Authentication Center | RADIUS | Remote Authentication Dial-in User Service |
| EAP | Extensible Authentication Protocol | SIM | Subscriber Identity Module |
| HLR | Home Location Register | WLAN | Wireless LAN |
| MSISDN | Mobil Station ISDN Number | | |

Das EAP AKA (RFC 3310) ist ein ähnliches Verfahren, das in einem UMTS-Netz genutzt wird. Auch hier ist seitens der WLAN-Endstelle der Einsatz einer USIM-Karte notwendig. Als Gegenstelle wird ebenfalls ein RADIUS-Server eingesetzt.

## Integrationsszenario 3: Zugriff auf gemeinsame Dienste

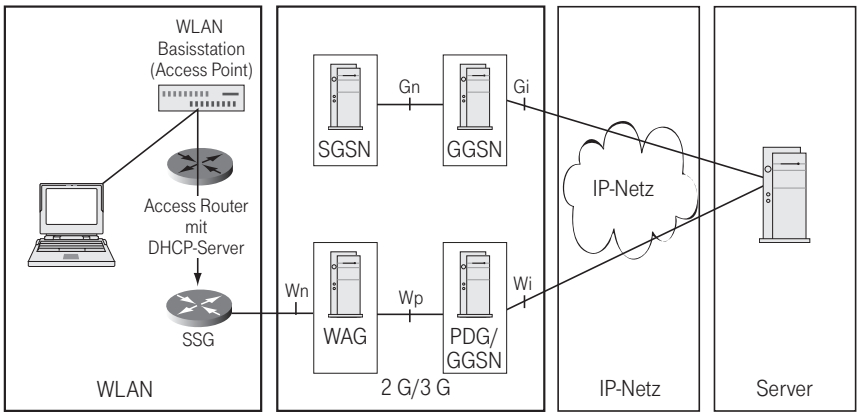
Das Standardisierungsgremium 3GPP beschreibt im aktuellen Referenzdokument TS 23.234 eine Architektur zur Integration von zellularen Mobilfunksystemen auf Basis von GSM oder UMTS und WLAN-Zugangssystemen. Diese Referenzarchitektur ist kompatibel zu allen bisherigen WLAN-Standards nach IEEE 802.11. Das bedeutet, dass vorhandene standardkonforme WLAN-Endstellen in zellulare Mobilfunknetze integriert werden können. Dies ist eine grundlegende Voraussetzung für den Markterfolg. Spezielle Änderung am IEEE 802.11 Standard (d. h. auf OSI-Schicht 2 und OSI-Schicht 1) würde die Einführung dieses Integrationsszenarios erschweren oder gar unmöglich machen. Obwohl die Standardisierung noch nicht abgeschlossen ist, stehen die grundlegenden Verfahren und Konzepte bereits fest.

Bild 5 zeigt den grundsätzlichen Aufbau der Referenzarchitektur, die eine deutliche Parallele zu 2,5-G-/3-G-Netzen aufweist. Das Packet Data Gateway nimmt hier die gleiche Rolle mit nahezu identischen Funktionen ein wie der GGSN und ist zuständig für das Interworking mit externen IP-Netzen. Hierunter fallen Funktionen wie Routing und, abhängig vom jeweiligen W-APN, die Zuweisung und/oder Übersetzung (Mapping) von IP-Adressen.

Die Frage der weitergehenden Integration von PDG und GGSN lässt der Standard offen und ist somit eine Design-Entscheidung der Implementierung. Optional sieht der Standard eine Schnittstelle Gn’ zwischen PDG und GGSN vor. In diesem Fall verhält sich das PDG aus Sicht des GGSN wie ein SGSN.

Die Wi-Schnittstelle entspricht der Gi-Schnittstelle der 2,5-G-/3-G-Architektur. Das WLAN Access Gateway (WAG) übernimmt in dieser

**Bild 5** **Integrationsszenario 3 – Dienstintegration**

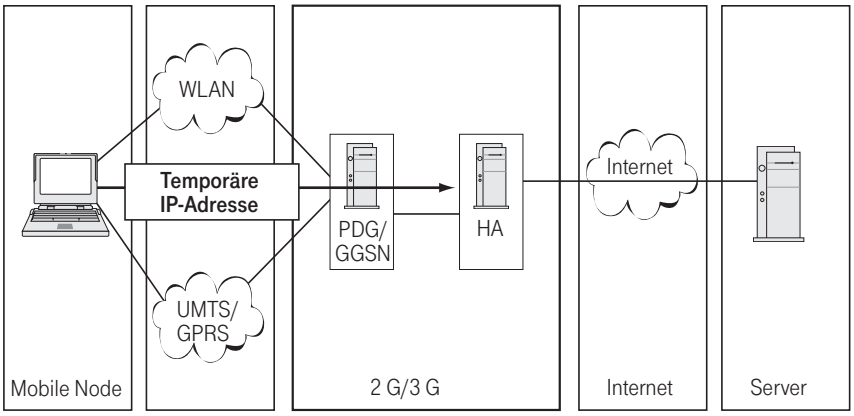



| | | | |
|---|---|---|---|
| DHCP | Dynamic Host Configuration Protocol | SGSN | Serving GPRS Support Node |
| GGSN | Gateway GPRS Support Node | SSG | Service Selection Gateway |
| Gn, Gi | Schnittstellenbezeichnung | WAG | WLAN Access Gateway |
| IP | Internet Protocol | WLAN | Wireless LAN |
| PDG | Packet Date Gateway | Wn,Wi,Wp | Schnittstellenbezeichnung |

Architektur die Rolle eines SGSN in einem fremden 2,5-G-/3-G-Netz (visited PLNM)[21]. Die Wp-Schnittstelle entspricht daher in ihrem Funktionsumfang der Gp-Schnittstelle im GPRS-Roaming-Fall. Die Wn-Schnittstelle zum WLAN-Zugangsnetz wird analog wie die Gn-Schnittstelle zwischen zwei SGSN eines 2,5-G-/3-G-Netzes ausgeführt.

Ein weiteres Konzept ist die Adressierung externer IP-Netze und externer IP-basierter Dienste über einen Access Point Name (APN). Das 3GPP spricht hier im Zusammenhang mit der Integration von WLAN und 2,5-G/3 G von einem W-APN. Der W-APN ist gleichfalls ein Domain-Name, der von einem Domain Name Server (DNS) in eine IP-Adresse eines PDG übersetzt wird, über welches das jeweilige externe IP-Netz angeschaltet ist. Mit diesem Konzept lassen sich über WLAN sowohl Server erreichen, die über das Internet angebunden sind, als auch private Unternehmensnetze, die über eine direkte Anschaltung an den GGSN oder das PDG verfügen.

**Bild 6** **Integrationsszenario 4 – Service Continuity mit Mobile IP**




| | | | |
|---|---|---|---|
| GGSN | Gateway GPRS Support Node | PDG | Packet Date Gateway |
| GPRS | General Packet Radio Service | UMTS | Universal Mobile Telecommunications Service |
| HA | Home Agent | WLAN | Wireless LAN |
| IP | Internet Protocol | | |

Auf der Basis der aktuellen Referenzarchitektur sind bereits Konzepte und erste Implementierungen vorhanden, die WLAN- und 2,5-G-/3-G-Verkehr in einem gemeinsamen PDG zusammenführen.

## Integrationsszenario 4: Service Continuity

Die beschriebene Referenzarchitektur des Integrationsszenario 3 erlaubt bereits den Zugriff auf gemeinsame IP-basierte Dienste oder IP-Netze. Ein unterbrechungsfreier Wechsel von WLAN zu UMTS oder umgekehrt ist damit jedoch noch nicht möglich. Erst mit Hilfe des Mobile IP (RFC 2002, RFC 3344) kann ein Teilnehmer aus einem WLAN-Hotspot beispielsweise über UMTS eine zuvor gestartete Anwendung ohne Neustart weiternutzen. Der komplizierte Wechsel der jeweiligen Zugangstechnik wird von ihm lediglich als eine kurze zeitliche Unterbrechung wahrgenommen. Diese Eigenschaft bezeichnet man als „Service Continuity“ (Bild 6).

Die wesentlichen Funktionen werden demnach vom so genannten Mobile Node (MN) und dem Home Agent (HA) erbracht. Der Mobile Node ist in der Regel Bestandteil eines Client-Programms auf der mobilen Teilnehmerendstelle, beispielsweise ein Laptop. Der Home Agent ist als Funktionselement neben oder als Bestandteil des GGSN oder PDG vorzusehen. Bei jeder Netzanmeldung, sei es über WLAN oder UMTS, verbindet sich der Mobile Node mit dem Home Agent und meldet sich unter seiner jeweils aktuellen temporären IP-Adresse an. Mit dieser Information kann der HA nun alle kommenden IP-Datenpakete, die an den betreffenden Mobile Node adressiert sind, an die temporäre IP-Adresse des Mobile Node weiterleiten. Verlässt nun ein Anwender mit seinem Laptop das Versorgungsgebiet eines WLAN-Hotspot, wird entsprechend des Integrationsszenario 3 die Netzverbindung beispielsweise über UMTS automatisch neu hergestellt. Anschließend aktualisiert der Mobile Node lediglich die temporäre IP-Adresse im Home

[21] Siehe hierzu den Beitrag „GPRS-Roaming in GSM-Netzen“, Unterrichtsblätter Nr. 8/2003, S. 456 ff.

Agent und ist von nun an erneut für externe IP-Pakete erreichbar. Während dieses Vorgangs wird der Anwender lediglich eine kurze Unterbrechung, jedoch keinen Abbruch auf Anwendungsebene wahrnehmen.

## Zusammenfassung und Ausblick

Ein WLAN bietet gegenüber GSM/GPRS oder UMTS wesentlich höhere Bandbreiten zu geringeren Kosten und erlaubt damit Anwendungen, die bislang nur in einem lokalen Netz oder über DSL lauffähig waren. Die räumliche Verfügbarkeit von WLAN ist jedoch auf wenige hundert Meter begrenzt.

Zellulare Mobilfunknetze wie GSM oder UMTS zeichnen sich demgegenüber durch eine große Netzabdeckung mit nahezu weltweiten Roaming-Möglichkeiten aus und bieten darüber hinaus anerkannt sichere Authentisierungs- und Übertragungsverfahren. Wireless LAN und zellularer Mobilfunk ergänzen sich daher gegenseitig. Für Mobilfunkbetreiber mit einer großen Kundenbasis sowie leistungsstarken Abrechnungs- und Customer-Care-Systemen ist eine Integration von WLAN-Hotspots und zellularem Mobilfunk von großem Interesse.

Obwohl die Standardisierung der hier vorgestellten Integrationsszenarien teilweise noch nicht abgeschlossen ist und noch viele technische Details ungeklärt sind, zeigt der aktuelle Stand der Technik deutlich, in welche Richtung die zukünftige Entwicklung gehen wird. Bereits heute gibt es beispielsweise von T-Mobile ein WLAN-Angebot, das nach dem Integrationszenario 1 über eine vorhandene Mobilfunkrechnung abgerechnet wird und von jedem Bestandskunden der T-Mobile als Zusatzangebot auf einfache Weise genutzt werden kann. Zudem sind bereits im Vorgriff auf einen abschließenden 3GPP-Standard für Szenario 3 erste Pilotimplementierungen verfügbar, die zeigen, dass eine enge Integration dieser sehr unterschiedlichen und hochkomplexen Zugangssysteme technisch möglich ist. Die langfristige Entwicklung wird zu einem eng integrierten System führen, das über alle mobilen Zugangswege eine sichere und zuverlässige Nutzung gemeinsamer IP-basierter Dienste ermöglicht, ohne dass sich der Kunde um die Komplexität der zu Grunde liegenden Technik kümmern muss. *(He)*

**Quellenverzeichnis**

[1] 3GPP TS 23.234

[2] Kalle Ahmavaara, IEEE Communications Magazine, November 2003, S. 74–81