# Interworking von UMTS und LAN: Eine sicherheitstechnische Betrachtung

K.M. Bayarou, S. Rohr und C. Eckert

Sichere Mobile Systeme
Fraunhofer Institut Sichere Telekooperation
Rheinstraße 75
D-64295 Darmstadt
{bayarou|rohr|eckert}@sit.fraunhofer.de

**Zusammenfassung:** Lange vor dem kommerziellen Start der UMTS Netze in Deutschland hatten Wireless LANs nach IEEE 802.11(b) ihren Durchbruch als kabelloser Netzzugang im Unternehmen, in den Hochschulen, zu Hause und auch an öffentlichen Plätzen. Vielfach wurde deshalb der kommerzielle Erfolg so genannter „Hotspots“, also öffentlich zugänglicher WLANs mit geringer Nutzungsgebühr, als Ursache für eine bevorstehende Totgeburt des auf paketorientierte Daten- und Sprachübertragung ausgelegten UMTS Netzes genannt. Neue Initiativen wie „Greenspot“, dem Clearinghouse Angebot des Verbandes der deutschen Internetwirtschaft sowie wissenschaftliche Ansätze zur Lösung der beim Roaming auftretenden Probleme (Vertrauens- bzw. Vertragsbeziehungen zwischen den einzelnen Hotspot-Betreibern und den Carriern) deuten auf die wirtschaftliche Relevanz des Themas zu hin. Da sich einzelnen Hotspots zwar durchaus kostengünstig etablieren lassen, eine flächendeckende Versorgung mit WLAN jedoch technologisch aufgrund der fehlenden Backboneinfrastruktur nicht erreichen lässt, wäre die konsequente Schlussfolgerung ein Interworking der beiden zu realisieren. Das UMTS Netz würde dann in der Fläche eine (etwas kostenintensivere und in der Bandbreite beschränkte) Versorgung mit Sprache und Daten garantieren, während an Hotspots die hohe Bandbreite und die geringen Gebühren einer IEEE 802.11 Nutzung Vorteile bei der Datenübermittlung ermöglichten. Das Interworking dieser grundverschiedenen Technologien wirft technische und wirtschaftliche Probleme auf, die aus der simultanen Nutzung beider Netze und einem Handover zwischen diesen resultieren. Von besonderer Wichtigkeit hierbei ist die Sicherheit für den Nutzer und dessen Endgerät, seine persönlichen Daten und vor allem die korrekte Abrechenbarkeit der Dienste- und Netznutzung bei diversen Anbietern. Konkret betreffen diese Probleme die zu verwendenden AAA Mechanismen (insbesondere Authentisierungsunterschiede zwischen WLAN und UMTS) sowie das Billing & Accounting bei der Inanspruchnahme des Netzzuganges oder der Mehrwertdienste unterschiedlicher Anbieter. Der Beitrag skizziert den derzeitigen Status der technischen Entwicklung zum WLAN-UMTS Interworking, stellt die Sicherheitsanforderungen und die derzeit verfügbaren und in Entwicklung befindlichen Authentisierungsmechanismen (u.a. 802.1x, EAP-TLS, EAP-AKA, EAP-SIM) vor und erläutert die bislang noch offene Sicherheitsprobleme.

## 1 Einleitung

Im Vorwege der Einführung von UMTS oder allgemein Mobilfunknetzen der dritten Generation (3G) wurde viel über die stark erhöhten Datenraten dieser Technologien und die damit möglichen mobilen Anwendungen gesprochen, selten jedoch wurden die daraus entstehenden Kosten für die Datenübertragung thematisiert. Da viele der heute mobil genutzten Anwendungen (Emails, Auftragsbearbeitung und -versand etc.) nicht unbedingt eine stetige Verbindung benötigen, sondern nach Bedarf „im Stapel“ genutzt und abgearbeitet werden, kann man diese auch mittels räumlich begrenzter WLAN Hotspots nutzen sobald diese in Reichweite kommen (Café, Restaurant, Hotellobby). Hierbei können sich Synergien bei der gleichzeitigen bzw. verzahnten Nutzung der Zugriffstechnologien ergeben. Damit diese Vorgänge ohne weiteres Eingreifen des Nutzers zur Authentisierung oder Auswahl ablaufen, sind weitgehende Vereinfachungen bei der Interaktion zwischen mobilem Endgerät, den betreffenden Zugangsnetzen und dem Nutzer notwendig. Diese Vereinfachungen dürfen jedoch keinesfalls zu Lasten der Sicherheit oder Privatsphäre durchgeführt werden, sondern müssen vielmehr dem Nutzer eine sichere Plattform für die Verrichtung seiner Tätigkeiten bieten. Hier setzt dieser Beitrag an und zeigt im Folgenden auf, welche Ansätze für eine Kopplung der WLAN- und Mobilfunknetze gegenwärtig diskutiert werden.

Die Verzahnung von WLAN und Mobilfunknetzen kann, wie in Abschnitt 3 erklärt wird, grundlegend auf verschiedenen technologischen Ebenen vorgenommen werden. Durch die erheblichen Unterschiede in den Netzarchitekturen der beiden Technologien ergeben sich also verschiedene Aspekte, die bei der jeweilig gewählten Methode der Kopplung unterschiedlich stark zur Wirkung kommen. Zum einen sind dies Probleme der Authentisierung, da sich die 3G (hier beispielsweise UMTS-) Technologie vollkommen auf (U)SIM basierte Mechanismen beschränkt, im WLAN Umfeld jedoch eine Vielzahl von Authentisierungsverfahren genutzt werden können. Angefangen von einfachen Nutzername/Passwort Verfahren bis hin zu komplexen, auf Zertifikaten basierenden Verfahren, wie Extensible Authentication Protocol – Transport Layer Security (EAP-TLS). Abgesehen von Abrechnung und Nutzungsberechnung (Billing & Accounting), befasst sich ein weiterer Problemkreis mit der Verschlüsselung der im Zugangsnetz übertragenen Nutz- und Management Daten. Im bisherigen Mobilfunknetz werden diese Daten über SIM-basierte bzw. providerinterne Schlüssel mit teilweise nicht öffentlichen Verfahren auf der Luftschnittstelle verschlüsselt. Es ist zwar teilweise gelungen diese Verfahren mit Brute Force Angriffen zu brechen, der potentielle Nutzen entsprach dem hierfür nötigen Aufwand jedoch nicht annähernd. Die Unsicherheit der WLAN internen Verschlüsselungsverfahren Wire Equivalent Privacy (WEP) und WiFi Protected Access (WPA) wurde hinlänglich in wissenschaftlichen Abhandlungen und Fachzeitschriften dargestellt und alle bislang zusätzlich entwickelten Erweiterungen haben ebenfalls Lücken gezeigt (z.B. CISCO Lightweight EAP LEAP) oder sind immer noch nicht endgültig verabschiedet ( IEEE 802.11i). Zudem basieren alle diese Verfahren auf der Bekanntheit eines gemeinsamen Geheimnisses (shared secret) oder dem Besitz eines Zertifikates (EAP-TLS) was bei der „zufälligen“ bzw. spontanen Nutzung eines Hotspots als nicht gegeben gesehen werden muss.

Diese Probleme stellen gleichzeitig die Herausforderungen dar, die beim Interworking zwischen UMTS und WLAN zu meistern sind. Im vorliegenden Beitrag werden Aspekte der Sicherheit, die zurzeit in Fachkreisen diskutiert werden, betrachtet.

Hierfür werden zunächst die Systemspezifischen Sicherheitsmechanismen und -probleme der beiden Technologien für sich betrachtet um anschließend detailliert die Anforderungen für ihr sicheres Zusammenspiel darzulegen. Insbesondere die Vorarbeiten des 3GPP (3rd Generation Partnership Project) werden hierbei berücksichtigt. Dabei sollen die Sicherheitsaspekte die Hauptrolle einnehmen und durch eine Betrachtung der 3GPP Lösungsansätze und einige bereits veröffentlichter Ansätze eine Rolle spielen. Einen Überblick über die Konzepte zur Integration von UMTS und WLAN wird gegeben.

Neben diesem ersten Kapitel gliedert sich dieser Beitrag in drei weitere Teile. Zunächst wird in Kapitel 2 auf die Sicherheitsmechanismen in UMTS sowie auf die aktuellen Sicherheitsstandards in IEEE 802.11 WLANs eingegangen. Im Kapitel 3 wird dann das Interworking von 3G und WLAN näher betrachtet, wobei die Sicherheitsanforderungen und die von der 3GPP entworfenen Interworkingszenarien und diverse Sicherheitsmechanismen fokussiert werden. Kapitel 4 gibt die Schlussbetrachtung sowie einen Ausblick auf die Vision des Future Net.

## 2 Sicherheitsbetrachtung von UMTS and WLAN

Die beiden Technologien UMTS und WLAN unterscheiden sich nicht nur hinsichtlich Architektur, Zweck/Nutzung, sondern auch hinsichtlich ihrer Sicherheitskonzepte. Deshalb ist es notwendig, zunächst getrennt die Sicherheitskonzepte, ggf. Schwachstellen und zugehörigen Lösungsansätze zu diskutieren, um anschließend eine für beide Netze nutzbare Lösung zu betrachten. Bei dieser Diskussion wird die Grundsätze des jeweiligen Konzeptes erläutert und auf die weiterführenden Quellen, in denen die Details nachgeschlagen werden können, hingewiesen.

### 2.1 Sicherheit in UMTS

Die zelluläre Mobilfunktechnologie UMTS baut maßgeblich auf dem seit vielen Jahren bewährten Konzept der GSM Technologie auf. Da es jedoch im Laufe der Jahre mehrere erfolgreiche Angriffe auf die zumeist geheimen Sicherheitsmechanismen bei GSM gegeben hat, wurden bei UMTS ausschließlich offene (bekannte) Algorithmen und Verfahren gewählt, die zudem über längere Schlüssellängen (als bei GSM üblich) verfügen. Ein besonderer Schwachpunkt der GSM Netze, nämlich die nur einseitige Authentisierung des Nutzers/der SIM gegenüber dem Netz, konnte durch eine beidseitige (mutual) Authentisierung im UMTS Netz behoben werden. Hierbei wird neben dem Nutzer auch das Netz authentisiert, in das sich der Nutzer einbuchen will.

#### 2.1.1 Beschreibung der Sicherheitsarchitektur des UMTS

Im Gegensatz zum weit verbreiteten GSM, in dem die meisten Sicherheitsfunktionen unter strenger Geheimhaltung spezifiziert und verabschiedet wurden, sind bei UMTS alle Spezifikationen und Evaluationsberichte öffentlich zugänglich, wodurch das Vertrauen in die

Systemsicherheit und deren Qualität erheblich gestärkt wird. Dennoch übernimmt UMTS einige Basis-Sicherheitsdienste aus GSM, unter anderem Systeme zur Vertraulichkeit der Teilnehmeridentität durch Nutzung der „Temporary Mobile Subscriber Identity“ TMSI an Stelle der IMSI. Als besonderes Analogon kann aber die Verwendung einer IC-Karte, die UMTS SIM (USIM) genannt wird, die weitgehend dieselben Funktionen wie eine SIM-Karte im GSM bereitstellt, darüber hinaus (im UMTS) jedoch einige zusätzliche Funktionen (z.B. die Authentisierung des Netzes gegenüber dem mobilen Gerät) bereitstellt. Als entsprechende Gegenstelle im Netzwerk fungiert sowohl im GSM als auch bei UMTS das Authentication Center (AC), das z.B. für die Erzeugung des Integritätsschlüssels IK zuständig ist. Um das Kernnetz (core network) und dessen Signalisierung zu schützen, würde für die verwendeten Mobile Application Part (MAP) Nachrichten eine Erweiterung vorgeschlagen (MAPSec), die IPSec ähnliche Headererweiterungen mit Sicherheitsinformationen an die Nachrichten anfügt. Neben der bereits erwähnten beiderseitigen Authentisierung von mobilem Gerät und Netzwerk kommen Sequenznummern zur Abwehr von Replayattacken zum Einsatz und Mechanismen zur Sicherung der Nachrichtenintegrität zur Anwendung. Ein besonderer Punkt bei der Sicherstellung der Systemintegrität ist die Benachrichtigung des Heimatnetzes über fehlgeschlagene Authentisierungsversuche. Hierdurch kann ein Maskierungsangriff eines nicht legitimen Netzes (etwa der Nutzung eines so genannten IMSI Catchers) aufgedeckt werden.

Die bereits angesprochene Authentisierung erfolgt mittels dem als Authentication and Key Agreement (AKA) genannten Verfahren, einem Challenge-Response Mechanismus, der einen zwischen AC und USIM geteilten geheimen Schlüssel K nutzt. Dieser wird bei der Erstellung der USIM durch den Betreiber des Netzes auf die USIM übertragen und verlässt diese nie. Im Laufe der Authentisierung werden die Authentifizierungsfunktionen f1 und f2 sowie die Funktionen f3, f4 und f5 zur Schlüsselgenerierung verwendet. Für die Herleitung des Schlüsselmaterials für Authentifizierung (AK), Verschlüsselung (CK) und Integritätsschutz (IK) etc. unter Verwendung von AKA sowie deren Verwaltung, wird auf [Ec03] und [3G04d] verwiesen.

### 2.1.2 Mögliche Schwachpunkte bei UMTS

Bisher gelten die UMTS Sicherheitsmechanismen als sicher – diese Aussage bezieht sich jedoch nur auf den Vergleich zu den bei GSM gebräuchlichen Sicherheitsmechanismen. Genau hier liegen jedoch auch potentielle Probleme bei der UMTS Sicherheit, da die Interoperabilität zwischen GSM und UMTS eine der wichtigsten Anforderungen bei der Spezifikation des UMTS war. Hier werden standardisierte Konvertierungsfunktionen benötigt, um die Sicherheitsmerkmale und Parameter einer GSM-Verbindung beim Roaming auf diejenigen einer UMTS-Verbindung abzubilden, und umgekehrt. Zu beachten ist es auch, dass die Sicherheit der UMTS-Protokolle fundamental darauf basiert, dass die sensitiven Daten der Authentifizierungsvektoren auf einen sicheren und vertrauenswürdigen Weg über das Core Netwerk ausgetauscht werden. Da dies unter UMTS über IP-Netze erfolgen wird, sind erhebliche Anstrengungen notwendig, um sowohl die Kommunikationspartner wechselseitig zu authentifizieren und einen sicheren Kanal zu etablieren [Ec03]. Gegenwärtig wird nach Lösungsansätze und Gegenmaßnahmen der hier beschriebene Pro-

bleme, die im Prinzip nicht an UMTS liegen, sondern an der Art wie man UMTS zusammen mit anderen Technologien anwenden möchte (beispielsweise mit WLAN), erforscht. Einige dieser Ansätze werden im Kapitel 3 beschrieben. In nächsten Abschnitt werden die Sicherheitsmechanismen in WLAN näher betrachtet.

### 2.2 Sicherheit in IEEE 802.11 WLAN

Aufgrund der Tatsache, dass unter den Oberbegriff WLAN u.a. auch Technologien wie Hiperlan/2, HomeRF oder in gewissen Fällen auch Bluetooth fallen, begrenzen wir diesen Beitrag auf die kommerziell erfolgreichen und weit verbreiteten WLAN nach Standard IEEE 802.11, in den Ausprägungen a, b und g. Diese drei Ausprägungen unterscheiden sich maßgeblich in der maximalen Übertragungsrate (11 MBit/s bei „b“ bzw. 54 MBit/s bei „a“ und „g“) sowie der verwendeten Übertragungsfrequenz (2,4 GHz bei „b“ und „g“ sowie 5GHz bei „a“). Hieraus ergibt sich eine Abwärtskompatibilität zwischen „b“- und „g“-Netzen, da diese im gleichen Frequenzbereich arbeiten jedoch unterschiedliche Modulierungstechniken nutzen. Hinsichtlich ihrer Sicherheitseigenschaften gleichen sich die drei Standards vollkommen, wobei es Ausnahmen bei der zur Verfügung stehenden Schlüssellänge des WEP Verfahrens gibt.

WLANs werden grundsätzlich in zwei verschiedenen Betriebsmodi genutzt, dem Infrastruktur Modus, in dem eine variable Anzahl an mobilen Geräten sich in einem fest etablierten kabellosen Netzwerk an fest installierten Access Points anmelden oder in einem Ad-Hoc Modus genannten Betrieb, bei dem sich mehrere mobile Geräte ohne Hierarchie und Access Points direkt vernetzen. Siehe dazu [Ro02] und [AI99] für detaillierte Informationen über die Betriebsarten. Dieser Beitrag betrachtet lediglich den am weitesten verbreiteten Infrastruktur Modus, der sowohl in Unternehmen, Heimnetzen als auch in Hotspots zur Anwendung kommt.

#### 2.2.1 Beschreibung der Sicherheit des WLANs

Während der Spezifikationsphase für IEEE 802.11 Netze [AI99] war die Vision, eine günstige Erweiterungsmöglichkeit für kabelgebundene Ethernet Firmennetze zu entwickeln. Hierbei wurde die Einfachheit der Installation und des Betriebes in den Vordergrund gestellt und Sicherheitsprobleme wurden kaum berücksichtigt. Was Sicherheit angeht waren die beteiligten Entwickler keine dedizierten Krypto-Spezialisten, so dass das im 802.11 Standard als „Wire Equivalent Privacy“ (WEP) beschriebene Verfahren zur Authentisierung der mobilen Stationen und Verschlüsselung der Daten heutzutage als durchweg unzureichend betrachtet wird. Die rasante Entwicklung vom Unternehmensnetz zum beliebten Zugangsmedium in öffentlichen Zonen und zu Hause konnte während der Standardisierung ebenfalls nicht antizipiert werden, so dass für diese heutigen Anwendungsformen keine passenden Sicherheitslösungen vorgesehen sind. Einige dieser Schwachpunkte werden im nächsten Abschnitt beschrieben. Es ist zu erwähnen, dass in Fachkreisen WEP keine besondere Rolle mehr spielt, vielmehr werden neuere Entwicklungen wie 802.1x, 802.11i betrachtet.

### 2.2.2 Schwachpunkte des WLANs

Die heutigen Einsatzbereiche für WLAN (Heimnetz, Hotspots, Funkbrücken etc.) gehen weit über das hinaus, wofür die IEEE 802.11 Technologie anfänglich konzipiert wurde. Neben der erheblichen Verbreitung von WLAN über Unternehmensgrenzen hinaus hat die relativ einfache Architektur der Übermittlung auf der Luftschnittstelle zu einer wahren Subkultur von WLAN Hackern geführt, die auf so genannten „War Driving Sessions" mit leicht modifizierten Laptops und WLAN Karten Stadtteile und Industriegebiete durchkreuzen um mittels Anbindung eines GPS Empfängers und geeigneter Kartensoftware den Standort und die Eigenschaften offener WLANs festzuhalten.

Hierbei stellen die standardmäßig ohnehin deaktivierte WEP Verschlüsselung oder die Nutzung von auf MAC Adressen basierender Authentisierung der Clients nur verhältnismäßig geringe Hürden dar. Durch passives Belauschen lassen sich auch solche WLANs finden, bei denen das sog. Advertisement des APs durch Broadcast der Service Set Identifier (SSID) deaktiviert wurde. Es reicht hierbei, durch einen einfachen passiven Scan die aktiven Kanäle zu finden und dann auf die erste Anmeldung eines berechtigten Notebooks zu warten. Die Verbindungsanfragen werden hierbei unverschlüsselt übertragen und enthalten die notwendige SSID Information, so dass nach einer Umkonfiguration der MAC Adresse des Angreifers auf eine abgehörte und zulässige MAC, dem Angreifer die Möglichkeit gegeben wird in dieses „versteckte" Netz einzudringen.

Eine Verschlüsselung mittels WEP bietet keine signifikant Verbesserung der Sicherheit, da mittlerweile automatisierte Tools existieren, welche die Schwachstelle der sich wiederholenden Initialisierungsvektoren ausnutzen, und voll automatisch schwache Pakete aus dem Datenstrom filtern um daraus den WEP Schlüssel zu errechnen. Die Schwachstellen des WLAN sind in der breiten Masse bekannt und diese werden unmittelbar mit der Schwachstellen der WEP assoziiert. Es ist zu erwähnen, dass in der Fachpresse diese Themen betont werden obwohl mittlerweile graduelle Verbesserungen und Zusatzprodukte entwickelt worden sind, die diese Schwachstellen beheben sollen. Im nächsten Abschnitte werden einige dieser Produkte kurz beschrieben.

### 2.2.3 Lösungsansätze gegen Schwachpunkte im WLAN

Der Verband der WLAN Hersteller, das WiFi Konsortium, hat einige Zeit nach Veröffentlichung der Angriffsimplementierung auf das WEP Verfahren das modifizierte WiFi Protected Access (WPA) Verfahren vorgestellt. Dieses arbeitet teilweise in Vorwegnahme des bisher nicht verabschiedeten 802.11i Standards für die Authentifizierung mit 802.1x (unterstützt EAP, RADIUS/Kerberos), und für die Integrität der Daten mit Mechanismen der automatischen Schlüsselrotation (TKIP: Temporary Key Integrity Protocol), die ein gezieltes Erraten (educated guess) des Schlüssels erschweren, da die Anzahl der Pakete mit schwachen Initialisierungsvektoren innerhalb eines Gültigkeitszyklus nicht ausreicht, um den WEP Schlüssel zu berechnen. Die eigentliche Schwäche des WEP-Verfahrens wird hiermit jedoch nicht behoben, denn auch WPA setzt für die Wahrung der Vertraulichkeit auf den schwachen RC4 StreamCipher. Die 802.1x Verfahren sind zudem über Man-in-the-middle Angriffe zu attackieren und die über TKIP angebotenen Methoden des

Message Integrity Check (MIC) sind ebenfalls als schwach zu bewerten. Insgesamt können bisherige Installationen jedoch wirksamer gegen Angriffe geschützt werden ohne neue Hardware installieren zu müssen.

Neben den internen 802.11 Mechanismen gibt es eine Reihe von weiteren Möglichkeiten, die je nach Hersteller, unterschiedliche Varianten zur Authentisierung und Verschlüsselung im WLAN bieten. Insbesondere sei hier wiederum 802.1x genannt, welches seinen Ansatz des „port-based access control“ im Zusammenspiel mit dem EAP (Extensible Authentication Protocol) Framework bei Geräten vieler Hersteller ohne volle WPA Unterstützung ausspielen kann.

Abbildung 1 zeigt grundsätzlich wie die portbasierte Zugangskontrolle funktioniert. Hierbei stehen jedem physikalischen Netzzugang zwei logische Zugänge gegenüber, ein kontrollierter und ein unkontrollierter Port. Solange keine erfolgreiche Authentisierung über eine EAP Methode am unkontrollierten Port vorgenommen wurde, bleibt der kontrollierte Port unautorisiert und lässt keinen Datenfluß zu. Am unkontrollierten Port sind nur solche Datenströme zulässig, die für einen Authentisierungsablauf notwendig sind.

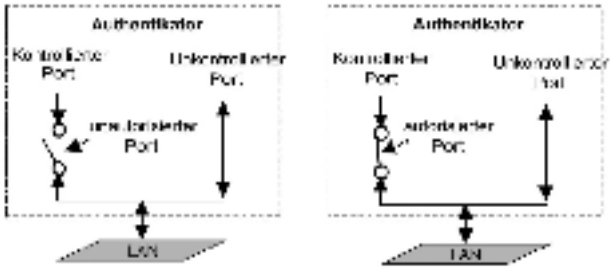


**Abbildung 1:** Portbasierte Zugriffskontrolle

Die Verwaltung über den Portzugriff hat der sogenannte Authentikator, welcher zwischen dem Supplicant (dem mobilen bzw. zu authentifizierendes Gerät) und dem Authentication Server (meist ein RADIUS oder Diameter Server) Pakete vermittelt. Der Authentikator „verpackt“ hierbei die Anfragen des Supplicant in EAPOL Pakete und übermittelt diese an den Server zur Verarbeitung (siehe Abbildung 2).

EAP selbst bietet jedoch nur ein Framework für die Einkapselung von Authentisierungsmethoden in EAP Pakete, die eigentlichen Methoden (etwa MD5, TLS, TTLS, LEAP) sind wiederum auswählbar und jeder Hersteller stellt andere Kombinationen in seinen Geräten zur Verfügung. Die große Auswahl an EAP Methoden beinhaltet sehr schwache (z.B. MD5) aber auch sehr gute und komplexe (z.B. TLS) Methoden, so dass im Vorwege einer Investition sehr genau auf die unterstützten EAP Typen geachtet werden sollte. Zwar müssen auch diese Methoden bei der heutigen Hardware Verschlüsselung auf das WEP Verfahren zurückgreifen, die Authentisierung erfolgt jedoch mittels Zertifikaten und jeder Client erhält pro Session einen eigenen Schlüssel. Somit wird die Wahrscheinlichkeit ausreichend Pakete mit schwachem IV (initial vector) abzufangen stark reduziert und soll-

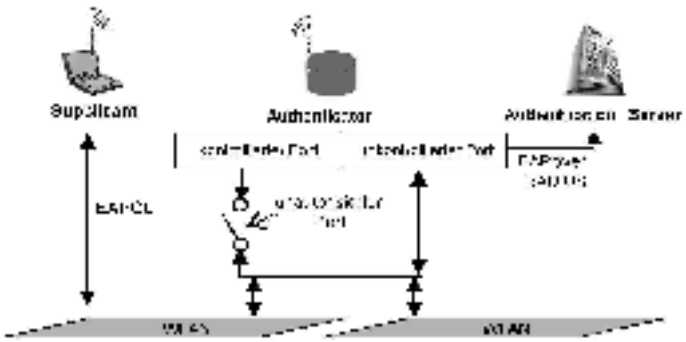

**Abbildung 2:** Rollen bei 802.1x

te es zu einer Kompromittierung kommen wäre nur die aktive Session des einen Client angreifbar. Die anderen Kommunikationspartner wären hiervon nicht betroffen und nach Beendigung der aktiven Session wäre auch der erratene Schlüssel nutzlos, da bei neuerlicher Verbindung ein neuer Schlüssel ausgehandelt wird. 802.1x bietet also neben den EAP Methoden zur Authentisierung auch ein Schlüsselmanagement an. Die Abbildung 3 zeigt den Zusammenhang zwischen 802.1x, WPA und dem 802.11i.

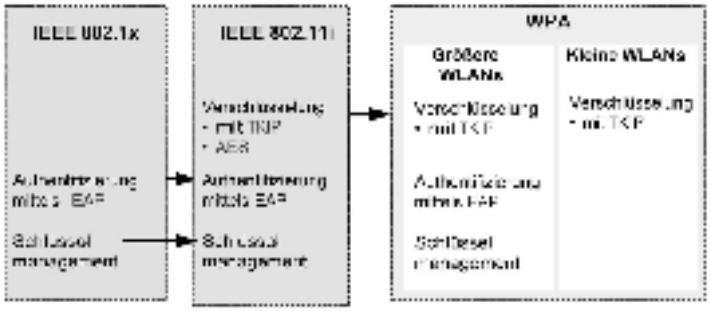


**Abbildung 3:** Zusammenhang zwischen IEEE 802.1x, IEEE 802.11i und WPA

Zukünftig wird in 802.11i-fähigen WLANs der Block-Cipher AES (Advanced Encryption Standard) zur Verschlüsselung verwendet. AES basiert auf dem Rijndael-Algorithmus, der selbst verschiedene Schlüssel- und Datenblocklängen erlaubt. AES schränkte diese jedoch auf verschiedene Schlüssellängen und Datenblöcke von 128 Bit ein.

Aus der Abbildung 3 wird ebenfalls ersichtlich, dass erst 802.11i mit AES eine wirklich neue Art der Verschlüsselung im WLAN erlauben wird. Diese AES Unterstützung erfordert neue Hardware, so dass bestehende Installationen erneuert werden müssen. Sowohl

WEP als auch WPA unterstützen nur den Infrastruktur Modus, während 802.11i auch im bisher vernachlässigten Ad-Hoc Modus genutzt werden kann.

Die aktuellen Lösungen mit 802.1x benötigen neben EAP auch einen zentralen Endpunkt, an dem die EAP Pakete entpackt werden und die Authentisierung durchgeführt werden kann. Dies wird allgemein mittels RADIUS abgewickelt.

Das Problem ist jedoch, dass RADIUS und EAP auf Layer 2 kommunizieren, was eine zentrale Abwicklung einer Authentisierung über die Grenzen eines Netzes hinaus (IP-Netze) stark erschwert. Für entsprechende Abhilfe können z.B. PANA (Protocol for carrying Authentication for Network Access) und DIAMETER eingesetzt werden, da diese auch Layer 3 Informationen verarbeiten und somit auch Authentisierungs-Informationen über Netzwerkgrenzen hinaus ermöglichen.

## 3 Interworking von UMTS and WLAN

Im Kapitel 2 wurden Sicherheitskonzepte in UMTS und im WLAN beschrieben und im Falle des WLAN wurden in großem Umfang neuere Konzepte erläutert, die die gegenwärtig bekannten Schwachstellen des WLANs schließen sollen. In diesem Kapitel werden die Konzepte zum Interworking zwischen UMTS und WLAN mit Akzentuierung auf die Sicherheitstechnik beschrieben. Da Begriffe wie Interworking unter Umständen unterschiedlich verstanden werden geben wir zunächst Erklärungen zu den im kommenden Abschnitt verwendeten Begriffen. Je nach Quelle wird der Begriff des Interworking sowohl als Roaming als auch Handover verstanden:

- Laut [3G02] wird erklärt, dass " ... the term interworking is used to express interactions between networks, between end systems, or between parts thereof, with the aim of providing an end-to-end communication".
- Als Handover wird " ... the process in which the radio access network changes the radio transmitters or radio access mode or radio system used to provide the bearer services, while maintaining a defined bearer service QoS." [3G03a] verstanden.
- Der Begriff Roaming wird auf zwei Weisen genutzt: einerseits ist es die Möglichkeit auch Netze von Betreibern (z.B. im europäischen Ausland) nutzen zu können, ohne dass man mit diesem Betreiber einen Vertrag abgeschlossen haben muss, und andererseits ist es die Eigenschaft, dass ein Teilnehmer von beliebigem Ort aus anrufen und dort auch angerufen werden kann, ohne dass dazu der mobile Teilnehmer seinen aktuellen Aufenthaltsort hinterlegen muss.

Für die Details der jeweiligen Auslegung wird jeweils auf angegebenen Quellen und [EB04] verwiesen. In diesem Betrag wird Interworking eher in Sinne des Handovers betrachtet, obwohl die zugrunde liegenden 3GPP Szenarien eher den Begriff des Roamings bevorzugen. Die Attraktivität eines Interworking zwischen UMTS und WLAN liegt vor allem in der Nutzung der Vorzüge der jeweiligen Technologie: bei UMTS ist dies die Reichweite und Netzabdeckung und bei WLAN die Bandbreite (siehe auch Abschnitt 1.1). Im nächsten Abschnitt werden Sicherheitsanforderungen, die bei einem Interworking sicherheitstechnisch zu erfüllen sind, beschrieben.

### 3.1 Sicherheitsanforderungen

Die Sicherheitsanforderungen, die für Interworking zwischen UMTS und WLAN festgelegt wurden, richten sich eng nach der UMTS Sicherheitsarchitektur, die bereits im Kapitel 2 beschrieben wurde. In Einzelnen wird folgendes verlangt: (1) Die Authentifizierungs-Maßnahmen müssen auf der Basis von Challenge Response Protokollen beruhen. (2) Alle langfristigen Sicherheits-Zeugnisse (credentials), die für den User und für die Netzwerkauthentifizierung verwendet werden, müssen auf UICC (Universal Integrated Circuit Card) oder SIM Card gespeichert werden. (3) Langfristige Sicherheits-Zeugnisse (credentials), die auf dem UICC oder SIM Card gespeichert worden sind, dürfen die UICC oder SIM Card nicht verlassen. (4) Gegenseitige Authentifizierung muss unterstützt werden. Und (5) EAP SIM und EAP AKA müssen vom AAA Server und dem WLAN UE (WLAN User Equipment) unterstützt werden.

Vergleicht man diese Anforderungen mit der oben beschriebenen UMTS Sicherheitsarchitektur, so erkennt man, dass der Versuch unternommen wird im Kontext des Interworking zwischen UMTS und WLAN die Schwachpunkte des WLAN zu umgehen und die gegenwärtig als stark eingeschätzte UMTS Sicherheit durchzusetzen. Dies soll wohl mit Hilfe des EAP Frameworks realisiert werden, indem EAP mit AKA bzw. EAP mit SIM kombiniert werden.

### 3.2 3GPP Szenarios

Die Bedeutung des Interworking zwischen Systemen mit größerer Reichweite (etwa UMTS) und solchen kürzerer Reichweite (WLAN) hat in jüngster Zeit zugenommen, so dass 3GPP die Initiative ergriff und eine Feasibility Study durchgeführt hat. Ziel dieser Studie ist es, mögliche Szenarien auszuarbeiten, die für das Interworking zwischen 3GPP spezifischen Systemen und WLAN in Frage kommen. Hierzu sei angemerkt, dass 3GPP nicht das gesamte IMT-2000 (das weltweit System der 3G laut ITU Festlegung) vor Auge hatte, sondern sich auf bestimmte Implementierungen beschränkt hat. Als Ergebnis dieser Studie sind insgesamt sechs Szenarien entstanden, die aufeinander aufbauen. Diese Szenarien werden im [3G03a] detailliert beschrieben. In diesem Dokument wird an bestimmten Stellen Hinweis auf diese Szenarien gegeben (siehe 3.4.1). Anhand der Ergebnisse der Feasibility Study hat 3GPP Dokumente zu Anforderungen [3G04a], Systembeschreibung [3G04b] und Sicherheit veröffentlicht. Zwar sind Szenarien [3G03b] durch 3GPP beschrieben und einige Anforderungen zu deren Einsatz formuliert, jedoch beschreibt das Dokument keine Realisierungsverfahren für die beschriebenen Szenarien. In Fachkreisen werden verschiedene Ansätze wie no, loose und tight coupling, diskutiert. Die Idee hinter dem loose coupling ist die Nutzung des WLAN als ein komplementäres Zugangsnetz zu dem bestehenden 3G Zugangsnetz. Bei tight coupling wird WLAN unter Nutzung des Iu Interface mit dem UMTS Corenet verbunden – ähnlich wie die anderen UMTS Zugangsnetze (UTRAN und GERAN).

Die Überlegung bei no coupling ist, dass keinerlei Kopplung zwischen UMTS und WLAN verlangt wird. Diese Art des Interworking hat Vorteile für die Hotspot Anbieter, die so in der Lage versetzt werden ihren Kunden UMTS Dienste anbieten zu können – vorausgesetzt der Hotspot liegt in der Reichweite eines UMTS Netzes und der WLAN Betreiber hat

mit dem UMTS Betreiber ein entsprechendes Abkommen abgeschlossen. Allgemein sinnvolle Kombinationen von Netzen wurden in [RB03] diskutiert. Zu Kopplungsarten mit 3G (nicht nur UMTS) und WLAN gibt es eine Reihe von Publikationen, jedoch wird [Sa04] empfohlen um einen Überblick zu bekommen.

In [EB04] wurden die Herausforderungen des Interworking im Hinblick auf QoS, AAA Sicherheit etc. ausführlich diskutiert.

### 3.3 Sicherheit in UMTS und WLAN Interworking

Wie im Kapitel 2 beschrieben, verfügen UMTS und WLAN über verschiedene Sicherheitskonzepte. Insbesondere wurden in großem Umfang die Probleme der WLAN Sicherheit und deren Lösungsansätze beschrieben. Dennoch stellt sich die Frage, wie das Sicherheitskonzept eines UMTS-WLAN Interworking aussehen soll? Welche Sicherheitsmechanismen können in diesem Kontext angewendet werden, so dass ein Anwender beim Wechsel von UMTS zu WLAN und umgekehrt den „höchst“ möglichen Sicherheitsschutz geniest? Es wird als Basis dieser Diskussion die 3GPP Spezifikation [3G04c] in der neuesten Version zugrunde gelegt. Es wird auf die wesentlichen Sicherheitsfeatures und Sicherheitsmechanismen Wert gelegt. Im Wesentlichen werden die Ansätze EAP AKA und EAP SIM betrachtet, da es zurzeit keine Sicherheitsarchitektur für das Interworking zwischen UMTS und WLAN existiert. Die im vorigen Abschnitt erwähnten unterschiedlichen Möglichkeiten zur Kopplung beider Netze erfordern bzw. beinhalten andere Sicherheitsrisiken und anderen Bedrohungspotentiale, sodass es weitere Überlegungen und Vorschläge gibt (siehe [EG04] und [BE04]). EAP AKA und EAP SIM können als Konzepte betrachtet werden, die in einer eventuellen Sicherheitsarchitektur zur Anwendung kommen. Die von 3GPP gegenwärtig ins Auge gefassten Sicherheitsfeatures sind die Vertraulichkeit und die Integrität. Es sind auch Aspekte der Privacy diskutiert worden, dennoch wird diese z.Z. nur auf der Ebene des jeweiligen Netzes behandelt.

#### 3.3.1 Einige Sicherheitsfeatures

Wie bereits erwähnt, konzentriert sich 3GPP auf Vertraulichkeit und Integrität. Es sind zur Authentifizierung des Subscribers und des Netzwerks sowie des Security Association Managements folgenden Forderungen gestellt: (1) End-to-End WLAN Access Authentifikation (Scenario 2). Dies muss auf Basis von Extensible Authentication Protocol (EAP) laufen, (2) Für den Transport der Authentifizierungs-Signalisierung über die WLAN Funk-Schnittstelle werden keine neuen Konzepte entwickelt, sondern IEEE 802.11i konforme Lösungen bevorzugt. (3) Zwischen UMTS und WLAN Schnittstelle wird der Transport der Authentifizierungs-Signalisierung auf Diameter oder RADIUS Basis gewährleistet. (4) Für User Identitätsschutz (Anonymität) werden temporäre Identitäten oder Pseudonyme verwendet. Zwar ist im EAP Kontext das PEAP (Protected EAP) (siehe Abschnitt 2) vorhanden, dennoch ist die Verwendung von PEAP mit EAP/AKA and EAP/SIM bisher nur in der Erprobungsphase.

Falls es zu einer Re-Authentifizierung beim WLAN Zugang kommt, wird eine 802.1x/AAA Kombination verwendet. Hierzu ist es anzumerken, dass es bei einer Re-

Authentifizierung auf eine komplette Ausführung des 802.11i aus Effizienzgründen verzichtet wird; es wird jedoch 802.1x genutzt (siehe Abbildung 3 im Kapitel 2). Der Prozess zur EAP SIM/AKA Re-Authentifizierung muss erst implementiert werden. Aus den Forderungen zur Vertraulichkeit und Integritätsschutz kann man anmerken, dass die Wiederverwendung der vorhandenen Protokolle das Ziel von 3GPP ist. Aus diesem Grund setzt 3GPP (mit Blick auf WLAN) auf die neuesten Entwicklungen wie 802.11i, 802.1x und Diameter.

### 3.3.2 Vertraulichkeitsschutz und Integritätsschutz

Für Vertraulichkeitsschutz und Integritätsschutz orientiert sich 3GPP nach der Anforderungen des jeweiligen Szenarios. Wie bereits erwähnt arbeitet 3GPP derzeit an den Details bis Szenario 3, daher werden nur die Unterschiede zwischen Szenario 2 und 3 dargestellt.

- **Zum Schutz der Vertraulichkeit und Integrität in Szenario 2** ist der Schutz der Vertraulichkeit/Integrität der Verbindungsschicht (link layer) im WLAN Zugangsnetz gefordert. Hierfür fühlt sich 3GPP jedoch nicht zuständig, da dies als WLAN spezifisch angesehen wird und von der WLAN Technologie abhängt. Im Falle von 802.11 WLAN müssen die Vertraulichkeits-/Integritätsmechanismen des IEEE 802.11i verwendet werden. Alle Schlüsselinformationen zwischen WLAN und dem Home Netzwerk (AAA Server) müssen vertraulich und integer (Vertraulichkeits- und Integritäts-Schutz) gesendet werden. Entsprechenden Mechanismen aus der WLAN Spezifikation kommen zur Anwendung.
  Es ist in “EAP AKA Authentication“ und “EAP SIM Authentication“ spezifiziert, wie das erforderliche Schüsselmaterial für die Vertraulichkeits-/Integritätsmechanismen der Verbindungsschicht von dem “Mastersitzungsschlüssel“ (master session Key) MSK abgeleitet wird. Die Generierung des MSK ist in EAP AKA Authentication“ und “EAP SIM Authentication“ definiert.
  Wenn die Schüsselherleitung (-Berechnung) im AAA Server beendet ist, dann wird das Schüsselmaterial an dem WLAN AN via Wa (WLAN – 3GPP AAA proxy) und Wd (3GPP AAA proxy – 3GPP AAA Server) Schnittstellen (im Fall des Roamings) gesendet.
- **Zum Schutz der Vertraulichkeit und Integrität in Scenario 3** muss es möglich sein die durch den Tunnel gesendeten IP Pakete vertraulich/Integrität geschützt zu versenden. Der Tunnel ist zwischen UE (User Equipment) und dem PDG (Packet Data Gateway) aufzubauen. An dieser Stelle ist es anzumerken, dass 3GPP eine neue Komponente, die als PDG genannt wird, eingefügt hat, um die paketorientierte Dienste des (PS Domains) über WLAN weiterzuleiten. Dieses Weiterleiten wird aus Sicherheitsgründen durch einen Tunnel gewährleistet.

Wenn die Vertraulichkeit/Integrität von IP Paketen, die durch den Tunnel zwischen dem UE und dem PDG gesendet werden, gefordert ist, müssen diese Pakete mit IPSec ESP nach RFC 2406 geschützt werden.

Aus Platzgründen wurde auf die 3GPP Roaming Modelle verzichtet, aus denen die Funktionalitäten des PDG und der in diesem Abschnitt genannten Interfaces (Wa und Wd)

zu entnehmen wären. Es wird für weitere Details auf die 3GPP Spezifikationsdokument [3G04b] verwiesen.

### 3.3.3 Authentifizierung und Schlüsselvereinbarung

In obigen Abschnitten wurden weitgehend Sicherheitsaspekte dargestellt, die aus der momentanen Entwicklung der 3GPP widerspiegeln: der Vertraulichkeitsschutz und der Integritätsschutz. Es ist wichtig zu wissen welche Methode wie selektiert wird und wie die entsprechende Schlüsselvereinbarung passiert. Es ist anzumerken, dass beide das WLAN UE und der AAA Server die EAP AKA und EAP SIM Methoden unterstützen. Die Prozedur um eine Methode zu selektieren lautet wie folgt:

1. Das WLAN UE muss eine Identität (welche immer das ist: permanent, pseudonym...) an den AAA Server senden. Wenn diese Identität eine IMSI (International Mobile Subscriber Identity) ist, dann muss sie einen Hinweis (indication) auf die EAP Methode, die zu verwenden ist, enthalten.
2. Wenn der AAA Server die EAP Methode erkennt, aber nicht die User Identität (z.B. ein obsoletes Pseudonym), dann muss er eine neue Identität unter Verwendung der durch das WLAN UE angezeigten EAP Methode anfordern
3. Wenn der AAA Server die User Identität erkennt (und infolgedessen die EAP Methode), dann sucht er nach AVs (Authentication Vectors) aus dem HSS (Home Subscriber Server).
4. Wenn die User Identität nicht erkannt wird, muss der AAA Server entscheiden, welche Methode zu verwenden ist (Es möge nur in dieser Situation eine „Defaultmethode“ ONLY existieren). Wenn diese Defaultmethode der User-Anmeldung nicht entspricht (z.B. EAP AKA für ein SIM User), dann muss das WLAN UE dem AAA Server mit einem NACK (not Acknowledged) antworten und der AAA Server muss es solange mit der anderen EAP Methode versuchen, bis eine bekannte Identität empfangen wird.

Unter der Annahme, dass eine richtige Methode EAP AKA oder EAP SIM selektiert ist, stellt sich die Frage was passiert mit der Methode d.h. wie wird sie angewendet. Der folgenden Abschnitten geben kürze Ablaufe beider Methoden.

### 3.3.4 EAP AKA und EAP SIM basierte Authentifizierung

Das Prinzip, auf dem beide Methoden basieren, ist relativ gut überschaubar. Die authentifizierende Komponente fordert die zu authentifizierende Komponente auf ihre Identität zu senden. Diese sendet ihre Identität zu der Authentifizierenden Komponente, welche die gesendete Identität überprüft. Bei einer erfolgreichen Überprüfung willigt die authentifizierende Komponente ein, dass die zu authentifizierende Komponente Zugang zu den gewünschten Ressourcen erhält. In den folgenden Abschnitten werden beide Methoden schematisch beschrieben.

#### 3.3.4.1 EAP/AKA basierte Authentifikation

Die Abbildung 4 zeigt den Informationsfluss des EAP AKA Authentifizierung. Die Abbildung ist quasi-selbsterklärend und wird daher nicht detailliert erläutert. Die Abfolgenummer wie 1, 4, etc., die keine Pfeile sind werden erklärt. In der Beschreibung wird auf die Nummer vorher Bezug genommen.

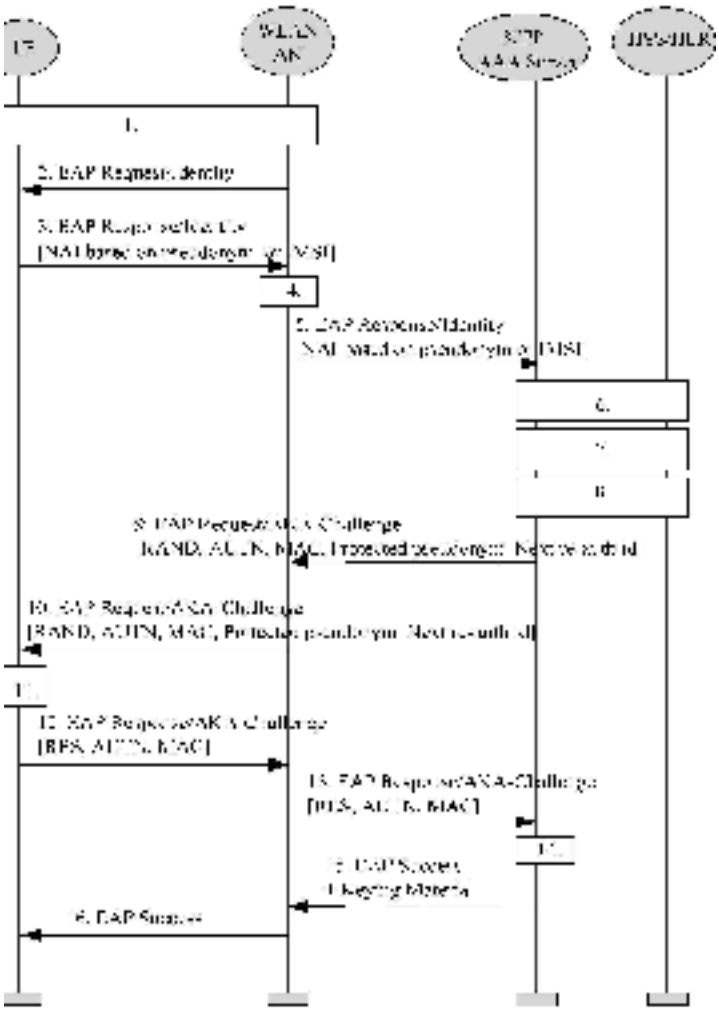

**Abbildung 4:** Informationsfluss innerhalb des EAP AKA Verfahrens

Erläuterung der Ablaufes der Authentifizierung auf der EAP AKA Basis:

1. Eine Verbindung wurde bereits zwischen dem WLAN UE und dem WLAN Netzwerk durch Verwendung WLAN Technologie spezifischen Prozedur (s. Kapitel 2) Etabliert.

4. Die Nachricht „EAP-Response“ wird unter Bezugnahme auf den Teil „Gebiet“ des NAI in Richtung des zuständigen 3GPP AAA Servers geführt. Der Routingpfad kann eine oder mehrere AAA Proxies beinhalten (Nicht in der Abbildung eingezeichnet). Hierzu können Diameter Empfehlungen verwendet werden, um den AAA Server zu finden.
6. 3GPP AAA Server identifiziert den Subscriber als einen Kandidaten für die Authentifizierung unter Verwendung von EAP-AKA, dies basierend auf der empfangenen Identität. Der 3GPP AAA Server überprüft dann, ob er einen vorhandenen unverbrauchten Authentifikationsvektor für den betreffenden Subscriber hat. Wenn dies nicht der Fall ist, fordert er neue Authentifikationsvektoren vom HSS/HLR an. Eine Zuordnung der temporären Identität auf die IMSI kann erforderlich sein.
7. 3GPP AAA Server überprüft, ob er für diesen Subscriber das WLAN Zugangsprofil hat. Wenn dies nicht der Fall ist, wird das Profil vom HSS angefordert. 3GPP AAA Server überprüft, ob der Subscriber berechtigt ist WLAN Dienste in Anspruch zu nehmen.
   Obwohl dieser Schritt nach dem Schritt 6 präsentiert ist, ist anzumerken, dass er irgendwo anders ausgeführt werden kann, jedoch nicht nach dem Schritt 14.
8. Neues Schüsselmaterial wird aus IK and CK wie es in EAP/AKA spezifiziert ist abgeleitet. Dieses Schüsselmaterial ist erforderlich für EAP-AKA. Weiteres Material kann auch für die WLAN Technologie spezifische Vertraulichkeits- und/oder Integritätsschutz generiert werden.
   Ein neues Pseudonym kann gewählt und geschützt werden (verschlüsselt und Integritätsschutz) durch Verwendung EAP-AKA generierten Schüsselmaterial.
11. Das WLAN-UE führt den UMTS Algorithmus auf der USIM aus. Die USIM überprüft, ob AUTN korrekt ist und hiermit authentifiziert (beglaubigt) er das Netzwerk. Falls AUTN nicht korrekt ist, weist der Terminal die Authentifizierung ab (nicht in dieser Abbildung). Falls die Sequenznummer nicht mehr stimmt, initiiert das Terminal eine Synchronisationsprozedur wie es in EAP-AKA spezifiziert ist. Falls AUTN korrekt ist, dann berechnet der USIM RES, IK and CK.
    Das WLAN UE leitet zusätzlich erforderliches Schüsselmaterial aus den von USIM neu berechneten IK and CK ab, überprüft die empfangene MAC anhand des neu berechneten Verschlüsselungsmaterials. Falls ein geschütztes Pseudonym empfangen worden war, dann speichert das WLAN-UE das Pseudonym für künftige Authentifizierungen ab.
14. 3GPP AAA Server überprüft den empfangenen MAC Wert und vergleich XRES mit dem empfangenen RES.

**EAP SIM basierte Authentifikation**

Die Abbildung 5 zeigt den Informationsfluss bei der EAP SIM basierte Authentifikation. Auch hier wird nicht jedem Schritt beschrieben, sondern die Schritte wie 1, 4 etc. Da einige wiederum identisch mit denen aus der EAP AKA sind, werden sie nicht noch einmal beschrieben. Eine entsprechende Referenz wird auf die EAP AKA wird angegeben. Schritte 1 und 4 sind genauso wie bei EAP AKA. Wie bereits erklärt läuft es ähnlich wie bei EAP AKA jedoch mit SIM Parameter. Es werden Schritte, bei denen es anderes Abläuft als bei EAP AKA und die nicht als selbsterklärend erscheinen, beschrieben.

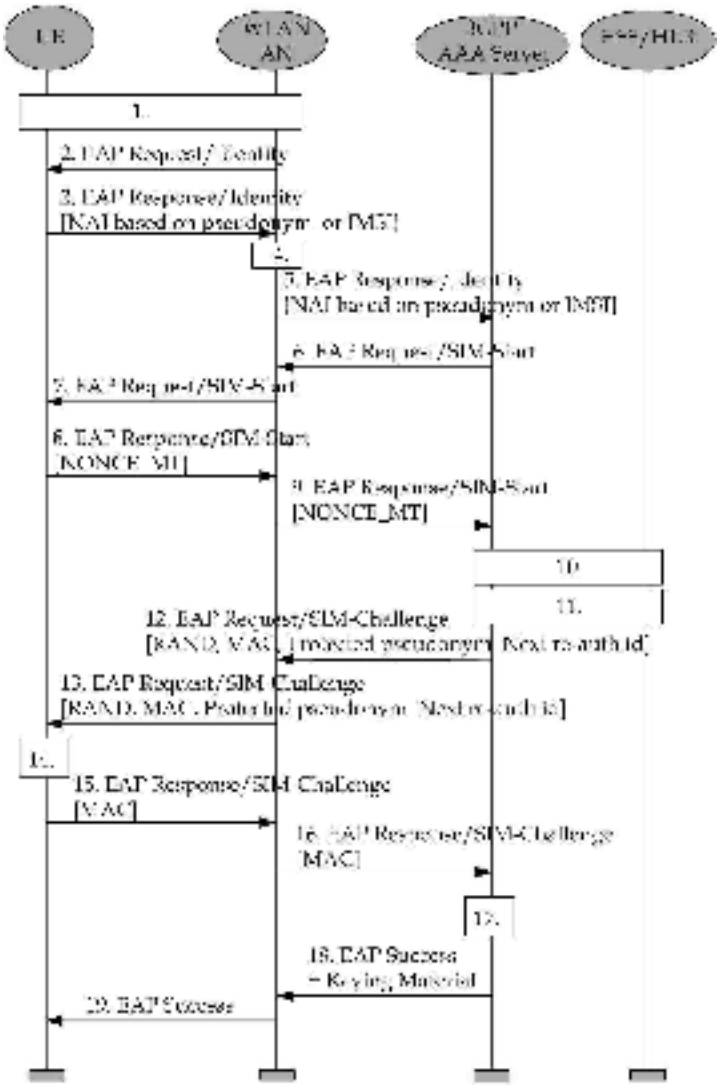


**Abbildung 5:** Informationsfluss innerhalb des EAP SIM Verfahrens

10. Das AAA Server überprüft, ob er N unverbrauchten Authentifizierungsvektoren für den betreffenden Subscriber hat. Mehrere GSM Authentifizierungsvektoren werden benötigt, um Schlüsselmaterial mit effektiver Länge äquivalent zu EAP AKA generieren zu können. Falls N Authentifizierungsvektoren nicht vorhanden sind, wird ein Satz(Menge) von Authentifizierungsvektoren von HSS/HLR angefordert. Eine Zuordnung der temporären Identität auf die IMSI kann erforderlich sein.

Obwohl dieser Schritt nach dem Schritt 9 präsentiert wird, ist es anzumerken, dass er irgendwo anders ausgeführt werden kann, beispielsweise nach dem Schritt 5, jedoch nicht nach dem Schritt 12.

14. WLAN-UE führt N Male den GSM A3/A8 Algorithmus auf der SIM-Karte (einmal für jede empfangene RAND) aus. Diese Berechnung ergibt N SRES und Kc Werte. Das WLAN-UE leitet zusätzliches Schlüsselmaterial aus N Kc Schüssel und NONCE_MT ab. Das WLAN-UE leitet seine Kopie des Netzwerk MAC mit Hilfe des neulich abgeleiteten Schlüsselmateriales ab und überprüft, ob sie dem empfangenen MAC Wert äquivalent ist. Falls der MAC Wert nicht korrekt ist, dann ist die Netzwerk-Authentifizierung verfehlt und WLAN-UE bricht die Authentifizierung (nicht in der Abbildung eingezeichnet) ab. Das WLAN-UE setzt den Authentifizierungsprozess fort nur wenn der MAC Wert korrekt ist. Das WLAN-UE rechnet einen neuen MAC Wert mit Hilfe des neuen Schüsselmaterials aus. Dieser MAC Wert umfasst EAP Message verkettet mit den N SRES Antworten. Falls ein geschütztes Pseudonym empfangen worden war, dann speichert das WLAN-UE das Pseudonym für künftige Authentifizierungen ab.
17. 3GPP AAA Server vergleicht seine Kopie des MAC Wertes mit dem empfangenen MAC.

Bemerkung: Die Herleitung des Wertes N wird weiter erforscht. D.h. zurzeit weiß man noch nicht genau wie hoch N sein soll.

### 3.3.5 EAP AKA und EAP SIM basierte Re-Authentifizierung

Wenn die Authentifizierungsprozesse oft auszuführen sind, kann es zu einer hohen Netzbelastung führen, besonders wenn die Anzahl der verbundenen User hoch ist. Dann ist es effizienter schnelle Re-Authentifizierungen durchzuführen. Somit ermöglicht die Re-Authentifizierung dem WLAN Netzwerk einen bestimmten User in einem schnellen Vorgang zu authentifizieren als im Voll-Authentifizierung (d.h. Authentifizierung von Anfang an). Dazu werden in der vorangegangenen Voll-Authentifizierung abgeleiteten Schlüssel (Identitäten) wiederverwendet. Aus Platzgründen wurde auf die Skizze des Re-Authentifizierung verzichtet.

Im Gegensatz zu Voll-Authentifizierung, bei der EAP AKA kürzer abläuft als der EAP-SIM, ist der Ablauf bei der Re-Authentifizierung sowohl bei EAP AKA als auch bei EAP SIM gleich. Ferner sind die Parameter, die bei der Re-Authentifizierung übergeben werden identisch. Es ist festzustellen, dass HSS/HLR in der Re-Authentifizierung nicht benötigt wird.

## 3.4 Schlussbetrachtung und Vision zur Future Internet

Konvergenz und Interoperabilität sind Schlagworte, die unabdingbar mit den vorangehend beschriebenen Technologien und Mechanismen einhergehen. Das angestrebte Interworking von heterogenen Netztechnologien wie sie durch UMTS und IEEE WLANs vertreten werden bietet einen weiten Raum bisher ungelöster Aufgaben, die einer wissenschaftlichen Betrachtung und Formalisierung bedürfen. Dieser Beitrag spiegelt nur einen

winzigen Bruchteil der angedachten Problemlösungen wieder, die zur Zeit in Standardisierungsgremien wie IEEE und 3GPP diskutiert werden. Die Verwendung der EAP Methoden AKA und SIM über Netzgrenzen hinweg werden von 3GPP als Authentifizierungsverfahren vorgeschlagen. Anstrengungen hinsichtlich der Kopplung von unabhängigen Hotspots mit Mobilfunknetzen der großen Operator stellen wiederum vollkommen andere Anforderungen an die anzuwendenden Mechanismen, insbesondere durch die fehlenden Vertrauensbeziehungen zwischen den beteiligten Parteien [EB04] [BE04].

Trotz dieser Hindernisse und Probleme ist die zunehmende Vernetzung unserer Umgebung und die Verquickung der dabei angewendeten Technologien unaufhaltsam. Ansätze des Ubiquitious Computing, Wearable Devices mit Kopplung durch Body- oder Personal Area Networks (BANs oder PANs) sowie die Umstellung auf leistungsfähigere Broadcasttechnologien wie DAB und DVB versetzen uns in die Lage auf immer vielfältigerem Wege Informationen zu sammeln, zu verteilen und auszuwerten. Um diese Vielzahl an Technologien bewältigen zu können bleibt als einziger Ausweg eine Vereinheitlichung, wie sie durch die angesprochenen Konvergenzbestrebungen erreicht werden kann. Hierzu wird die Weiterentwicklung von selbstkonfigurierenden Netzen, anpassbaren und adaptiven Wireless Schnittstellen (Software Defined Radio SDR) sowie die Anbindung von Sensor- und Ad-Hoc-Netzen beitragen. Alle bisher eher einzeln zu betrachtenden Forschungsbereiche zeigen Tendenzen, die umfassende Konvergenz und Interoperabilität als gemeinsames Fernziel sichtbar machen. Es ist noch nicht absehbar welche geeigneten Sicherheitskonzepte hierzu entwickelt werden können.

Um dieses (bisher rein akademische) Fernziel realisierbar zu machen besteht schon heute ein erhöhter Handlungsbedarf bei Industrie, Öffentlicher Hand und den Forschungsinstituten, um für die neu entstehenden Geschäftsmodelle und -ideen robuste und vertrauenswürdige Sicherheitsschutzmechanismen zu entwickeln und damit die Akzeptanz bei Verbrauchern und Geschäftspartnern zu erhöhen.

## Literatur

[AI99] ANSI/IEEE: Part 11 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) SpecificationsANSI/IEEE Std 802.11, 1999 Edition.

[Ro02] Roth J. Mobile Computing Grundlagen, Technik, Konzepte, dpunkt.verlag 2002.

[3G02] 3GPP: Core Network General network interworking scenarios TS 49.001 V5.0.0 (2002-06).

[Ec03] Eckert C., IT-Sicherheit: Konzept, Verfahren, Protokolle, 2. überarbeitete und erweiterte Auflage, Oldenbourg Verlag München Wien, 2003.

[3G03a] 3GPP: Handover Requirements between UTRAN and GERAN or other Radio Systems (Rel. 6) 3GPP TS 22.129 V6.0.0 (2003-03).

[3G03b] 3GPP: Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking (Rel. 6) TR 22.934 V6.2.0 (2003-09).

[RB03] Rohr S., Bayarou K. M., Eckert C., Prasad A.R., Schoo P., Wang H.: Feasible and Meaningful Combinations of Access and Network Technologies for Future Mobile Communications Conference: WWRF 10 in NY October 27-28, 2003.

[EB04] Eckert C., Bayarou K. M., Rohr S.: NGN, All-IP, B3G: Enabler für das Future Net?! Überblick über Entwicklungen im Bereich zukünftiger Netze In (GI Informatik-Spektrum, Band 27 Heft 1, Weber H. Hrsg.), Februar 2004 pp. 12-34.

[EG04] Enzmann M., Giessler E., Haisch M., Hunter B., Ilyas M., Schneider: A Note on Certification Path Verification in Next Generation Mobile Communications ACARS04 erscheint In Lecture Notes in Computer Science, Springer Verlag 2004.

[WP04] Wang H, Prasad A.R., Schoo P., Bayarou K. M., Rohr S: Security Mechanisms and Security Analysis: Hotspot WLANs and Inter-Operator Roaming VTC 2004 Spring, May 2004.

[BE04] Bayarou K. M., Enzmann M., Giessler E., Haisch M., Hunter B., Ilyas M., Rohr S, Schneider: Towards Certicate-based Authentication for Future Mobile Communications“ erscheint (In Kluwer Special Issue of Wireless Personal Communications on Security for Next Generation Mobile Networks).

[3G04a] 3GPP: Requirements on 3GPP system to Wireless Local Area Network (WLAN) interworking; 3GPP TS 22.234 V6.0.0 (2004-03).

[3G04b] 3GPP: 3GPP system to Wireless Local Area Network (WLAN) interworking; System description 3GPP TS 23.234 V6.0.0 (2004-03) (Rel. 6).

[3G04c] 3GPP: 3G Security Wireless Local Area Network (WLAN) Interworking Security (Rel. 6) 3GPP TS 33.234 V1.0.1 (2004-02).

[3G04d] 3GPP: 3G Security; Security architecture; 3GPP TS 33.102 V6.1.0 (2004-06) (Rel. 6).

[Sa04] Salkintzis A. K.: Tutorial on WLAN/3G Interworking, VTC 2004 Spring, Milan, Italy, May 2004.