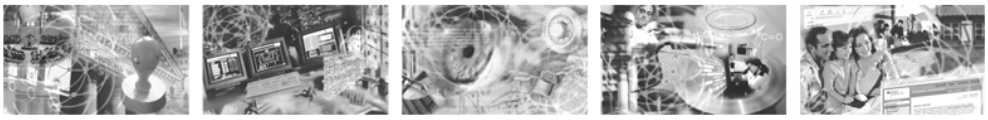
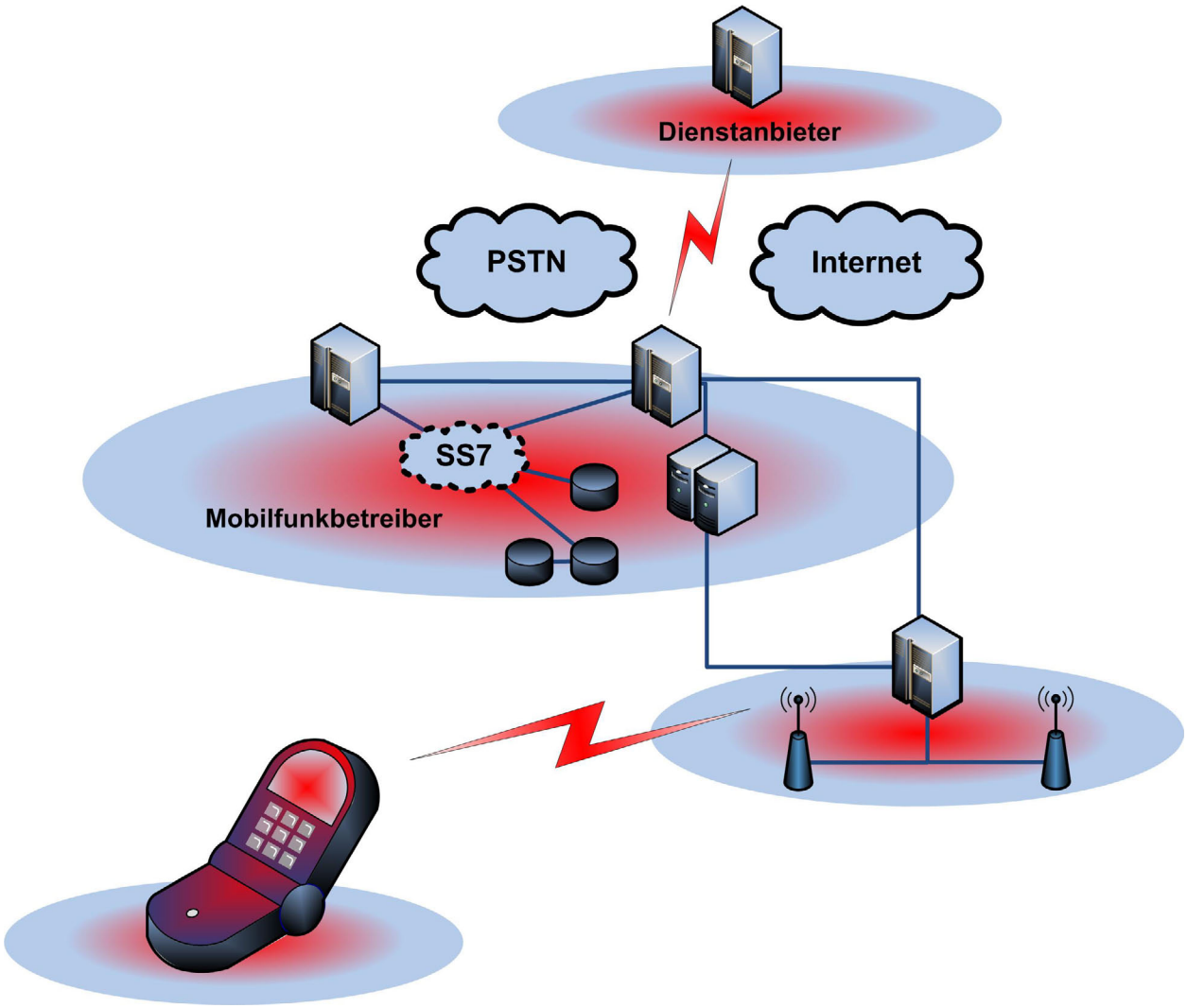
Bundesamt
für Sicherheit in der
Informationstechnik



Öffentliche Mobilfunknetze und ihre Sicherheitsaspekte



Diese Broschüre beschreibt die Funktionsweise von öffentlichen Mobilfunknetzen und ihre Sicherheitsaspekte. Sie zeigt mögliche Gefährdungen der Informationssicherheit bei Nutzung dieser Systeme auf und nennt Gegenmaßnahmen, welche zum Schutz vertraulicher Daten ergriffen werden können. Das Dokument reflektiert den Stand der Technik bis April 2008. An der Erstellung waren folgende Mitarbeiter des BSI (Bundesamt für Sicherheit in der Informationstechnik) beteiligt: Heinz Gerwing, Guido Reckhaus und Berthold Ternes. Weiterhin haben folgende Mitarbeiter der ComConsult Beratung und Planung mitgewirkt: David Ferrest, Dr. Simon Hoff, Dietlind Hübner, Dr. Frank Imhoff, Michael van Laak, Dr. Behrooz Moayeri, Nick Schirmer, Dr. Michael Wallbaum, Dr. Joachim Wetzlar und Dominik Zöller.

Bundesamt für Sicherheit in der Informationstechnik

Postfach 20 03 63

53133 Bonn

Tel.: +49 (0) 22899 9582 - 0

E-Mail: publikationen@bsi.bund.de

Internet: http://www.bsi.bund.de

Gliederung

Abbildungsverzeichnis

Tabellenverzeichnis

Einleitung

Die Nutzung öffentlicher Mobilfunknetze gehört für die meisten Europäer mittlerweile zum Alltag. Das immer noch steigende Kommunikationsaufkommen und die zunehmende Nutzung von kommerziellen Mobilfunkdiensten wie etwa M-Commerce (Mobile-Commerce) werfen die Frage der Datensicherheit innerhalb der öffentlichen Mobilfunknetze auf. Diese Broschüre beleuchtet daher existierende und zukünftige Mobilfunktechnologien in Bezug auf ihre Sicherheit.

Im Folgenden werden die zugrundeliegenden Übertragungstechnologien, grundlegende Netzarchitekturen sowie eingebaute Sicherheitsmechanismen der Netze beschrieben. Neben den technischen Grundlagen werden Sicherheitsgefährdungen beschrieben und Maßnahmen aufgezeigt, mit deren Hilfe man den Sicherheitsbedrohungen im privaten und kommerziellen Umfeld begegnen kann. Die Broschüre befasst sich dabei mit folgenden Technologien:

- Global System for Mobile Communications (GSM)
- General Packet Radio Service (GPRS)
- High Speed Circuit Switched Data (HSCSD) und Enhanced Data Service for GSM Evolution (EDGE)
- Universal Mobile Telecommunications System (UMTS)
- High Speed Downlink Packet Access (HSDPA) und High Speed Uplink Packet Access (HSUPA)
- High Speed Orthogonal Frequency Division Multiplex Packet Access (HSOPA)
- Satellitengestützte Mobilfunknetze

Über die Zugriffs- und Vermittlungsebene hinaus werden grundlegende Telefondienste, Multimedia- und Datendienste sowie in mobilen Netzen angebotene Mehrwertdienste auf ihre Sicherheitsaspekte hin beleuchtet. Beispiele hierfür sind:

- Short Message Service (SMS)
- Multimedia Message Service (MMS)
- M-Commerce
- Location Based Services

Die Kapitel 14 bis 16 geben abschließend einen Überblick über die Sicherheitsaspekte mobiler Endgeräte. Dabei werden allgemeine Sicherheitsfragen zum Umgang mit Endgeräten ebenso beleuchtet wie die gängigsten Schnittstellen und die auf mobilen Endgeräten eingesetzte Software. Unter anderem wird die zunehmende Bedrohung von mobilen Endgeräten und Datendiensten durch Schadprogramme thematisiert. Schwerpunkt des Dokuments ist neben der Sicherheit vertraulicher Informationen aus dem kommerziellen Umfeld der Schutz persönlicher Daten und der Privatsphäre.

1. Global System for Mobile Communications

Ursprünglich benannt nach der Groupe Spéciale Mobile, steht GSM heute für Global System for Mobile Communications und bezeichnet den weltweit meistverbreiteten Standard für digitale Mobilfunknetze.

Dieses Kapitel beschreibt die wichtigsten Sicherheitsaspekte innerhalb von GSM und stellt mögliche Bedrohungen sowie, falls vorhanden, geeignete Gegenmaßnahmen dar. Dabei wird GPRS zunächst explizit ausgenommen, da die Betrachtung erst im nächsten Kapitel erfolgt. Die für das Verständnis dieser Beschreibung notwendigen technischen Grundlagen werden im Vorfeld kurz erläutert.

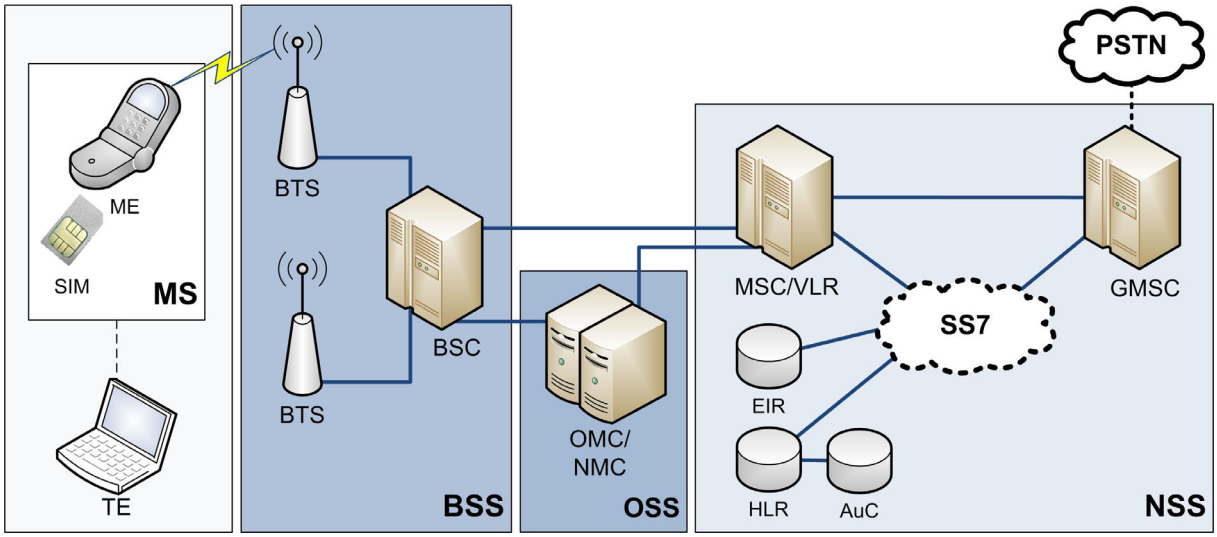
1.1 Technische Grundlagen

In diesem Abschnitt wird zunächst der Aufbau eines GSM-Netzes (ohne GPRS) dargestellt. Anschließend erfolgt eine Beschreibung der implementierten Sicherheitsfunktionen zur Authentisierung und Verschlüsselung innerhalb dieses Netzes.

1.1.1 Komponenten

Die im Rahmen dieses Dokumentes relevanten Elemente innerhalb eines GSM-Netzes (ohne GPRS) sind in Abbildung 1 dargestellt.

Abbildung 1: Vereinfachte Darstellung eines GSM-Netzes ohne GPRS



Ein GSM-Netz ist in vier Teilsysteme unterteilt, welche im Folgenden kurz beschrieben werden. Dabei handelt es sich um die Mobile Station (MS), das Base Station Subsystem (BSS), das Operations and Support System (OSS) und das Network Subsystem (NSS).

Das mobile Endgerät (Mobile Station, MS) besteht in der Regel aus einem Mobiltelefon (Mobile Equipment, ME) und einer SIM-Karte (gegebenenfalls mit angeschlossenem Terminal TE). Das Subscriber Identity Module (SIM) beinhaltet einen Prozessor und einen eigenen Speicher. Auf dem SIM werden Identitätsinformationen des Inhabers sowie weitere Daten

gespeichert, beispielsweise Adressbuchdaten oder Kurznachrichten. Insbesondere enthält das SIM ein nur mit dem zugehörigen Mobilfunkbetreiber geteiltes Geheimnis (englisch shared secret), welches nicht direkt auslesbar ist, sondern innerhalb der ebenfalls auf dem SIM gespeicherten Algorithmen zur Authentisierung und Verschlüsselung verwendet wird. Für weitere Informationen über die auf dem SIM gespeicherten Identitätsinformationen sowie die internen Krypto-Algorithmen siehe Kapitel 1.2.1 und Kapitel 1.2.2.

Das mobile Endgerät integriert sich in das GSM-Netz, indem es über die Luftschnittstelle eine Verbindung mit einem Base Station Subsystem (BSS) aufbaut. Nach Einschalten verbindet sich das mobile Endgerät mit dem Providernetz. Hierzu wählt die Betriebssystemsoftware einen verfügbaren Provider nach einer benutzerdefinierten Prioritätsliste. Dann baut das Endgerät eine Verbindung zur Zelle mit der höchsten Empfangsleistung auf. Das Endgerät befindet sich nun im Bereitschaftsmodus (Status „Idle“). Nun wird der Benutzer zur Eingabe einer Personal Identification Number (PIN) aufgefordert, anhand derer er sich gegenüber der SIM-Karte als berechtigter Nutzer authentifiziert. Im Folgenden dienen die auf der SIM-Karte gespeicherten Identitätsinformationen als virtuelle Identität des autorisierten Nutzers. Anhand dieser Daten wird die Anmeldung des Endgerätes am Providernetz durchgeführt. Bei Erfolg gilt das Endgerät als verbunden (Status „Connected“) und kann vom Benutzer verwendet werden. Der Wechsel zwischen Funkzellen ist sowohl im Bereitschaftsmodus (Cell Reselection) als auch im verbundenen Modus (Handover) möglich.

Um eine flächendeckende Verfügbarkeit eines Netzbetreibers bieten zu können, werden entsprechend viele Mobilfunksendesysteme benötigt. Ein Mobilfunksendesystem besteht in der Regel aus mehreren Sende- und Empfangsstationen (Base Transceiver Station, BTS) sowie einem Base Station Controller (BSC). Die Summe aller BSS bildet das GSM-Funknetz GSM EDGE Radio Access Network (GERAN). Jedes dieser Systeme ist mit dem Vermittlungssystem des jeweiligen Netzbetreibers verbunden.

Sämtliche Kommunikation des mobilen Endgerätes hinsichtlich Authentisierung, Gesprächsaufbau, Datenübermittlung usw. läuft über das Network Subsystem (NSS). Dies betrifft alle Gespräche – unabhängig davon, ob das Ziel ebenfalls ein mobiler Teilnehmer innerhalb des Betreibernetzes, sich der Teilnehmer in einem fremden Netz befindet oder ob es sich um einen Festnetzanschluss handelt.

Verbindungen innerhalb desselben Netzes werden über das Mobile Switching Center (MSC) vermittelt. Verbindungen aus dem internen Netz heraus, beispielsweise in das Festnetz (Public Switched Telephone Network, PSTN), werden über ein Gateway-MSC (GMSC) vermittelt. Die Kommunikation innerhalb des NSS läuft über ein Signalling System Number 7 (SS7) Netz. SS7 bezeichnet eine Reihe von Protokollen und Verfahren für die Signalisierung in Telekommunikationsnetzen.

Das Home Location Register (HLR) beinhaltet das vollständige Kundenverzeichnis eines Netzbetreibers und enthält sämtliche benötigten Informationen über die zugehörigen mobilen Teilnehmer, insbesondere

- die weltweit eindeutige Identität des mobilen Teilnehmers, die International Mobile Subscriber Identity (IMSI), die Telefonnummer der SIM-Karte, die Mobile Station ISDN Number (MSISDN) und

- Informationen über den aktuellen Aufenthaltsort des mobilen Teilnehmers.

Die Location Area Identity (LAI) kennzeichnet den Funkzellenverbund, Location Area, in dem sich der Mobilfunkteilnehmer aktuell befindet. Die LAI wird im Visitor Location Register (VLR) und auf der SIM-Karte gespeichert. Das VLR ist für die Mobilitätsverwaltung der Teilnehmer verantwortlich. Die Datenbank des VLR beinhaltet unter anderem die LAI des aktuell verwendeten Funkzellenverbandes. Diese Information wird benötigt, um ankommende Anrufe für den mobilen Teilnehmer dem richtigen BSC zuzuweisen, damit dieser das Gespräch durchstellen kann. Erst wenn z. B. ein Gespräch durchgestellt werden muss, wird ermittelt, über welche BTS eine Verbindung zur Mobilen Station (MS) besteht. Bei einem Wechsel in eine andere Location Area wird die LAI angepasst.

Ein VLR enthält Informationen über sämtliche aktiven Teilnehmer innerhalb von Funkzellen, welche über dasselbe MSC vermittelt werden. Daneben werden weitere Informationen des Teilnehmers im VLR abgelegt, wie z. B. IMSI, TMSI (Temporary Mobile Subscriber Identity) und Authentifizierungsdaten. Diese Informationen werden aus dem jeweils zugehörigen HLR kopiert bzw. mit diesem abgeglichen. Somit wandern die für die Vermittlung notwendigen Informationen mit dem Teilnehmer, wodurch lange Anfragewege bis zum zugehörigen HLR entfallen. Deutlich regelmäßiger als mit dem HLR kommuniziert das VLR mit dem zugehörigen MSC, da das MSC alle benötigten Informationen direkt aus dem VLR entnimmt. Kurze räumliche Distanzen und schnelle Kommunikationswege zwischen VLR und MSC sind also erstrebenswert. Daher ist das VLR in der Regel nur als alleinstehende logische Instanz zu sehen, da es meistens als Teil des MSC implementiert wird.

Das Authentication Center (AuC) ist eine geschützte Datenbank mit entsprechenden Methoden zur Teilnehmerauthentisierung und zur Berechnung von Sitzungsschlüsseln. In dieser Datenbank wird pro Kunde im zugehörigen HLR ein Shared Secret gespeichert, welches ebenfalls auf der SIM-Karte des Teilnehmers abgelegt ist. Dieses Shared Secret wird im Rahmen der Teilnehmerauthentisierung während der Ausführung der Algorithmen A3 und A8 benötigt (siehe Kapitel 1.1.4).

Optional kann innerhalb des NSS ein Equipment Identity Register (EIR) geführt werden, welches eine Liste aller gültigen bzw. zugelassenen mobilen Geräte enthält. Die Geräte werden über ihre zugehörige International Mobile Equipment Identity (IMEI) Nummer identifiziert. Es können drei Datenbanken verwaltet werden:

- Whitelist – alle bekannten und zugelassenen IMEIs
- Blacklist – nicht zugelassene IMEIs (z. B. als gestohlen gemeldete Geräte)
- Greylist – enthält zu prüfende IMEIs (Kandidaten für die Blacklist)

Die Implementierung eines EIR zur Sperrung von Geräten ist jedoch nicht als zuverlässig zu bewerten, da es Möglichkeiten gibt, die IMEI eines Mobilfunkgerätes zu ändern. Ebenfalls wird in der Regel bei einem Providerwechsel auch ohne Änderung der IMEI ein beim vorigen Provider gesperrtes Mobilfunkgerät wieder funktionieren, da nicht alle Provider ein EIR implementiert haben und – falls doch – diese in der Regel nicht untereinander synchronisiert werden.

Die Kontrolleinheit (Operations and Support System – OSS) ist sowohl mit dem BSS als auch mit dem NSS gekoppelt und stellt Funktionalitäten zum Betrieb und zur Überwachung des GSM-Netzes bereit. Das OSS beinhaltet (mindestens) ein Operation and Maintenance Center (OMC) sowie ein Network Management Center (NMC). Über das OSS erfolgen unter ande-

rem die Konfiguration sämtlicher GSM-Netzkomponenten sowie die Schaltung von Gesprächsüberwachungsfunktionen (englisch lawful interception). Das NMC bündelt alle vorhandenen OMCs, die jeweils meist nur für eine bestimmte geografische Region zuständig sind, und ermöglicht so das gesamte Netz zentral zu verwalten.

1.1.2 Funktionsweise und Protokolle

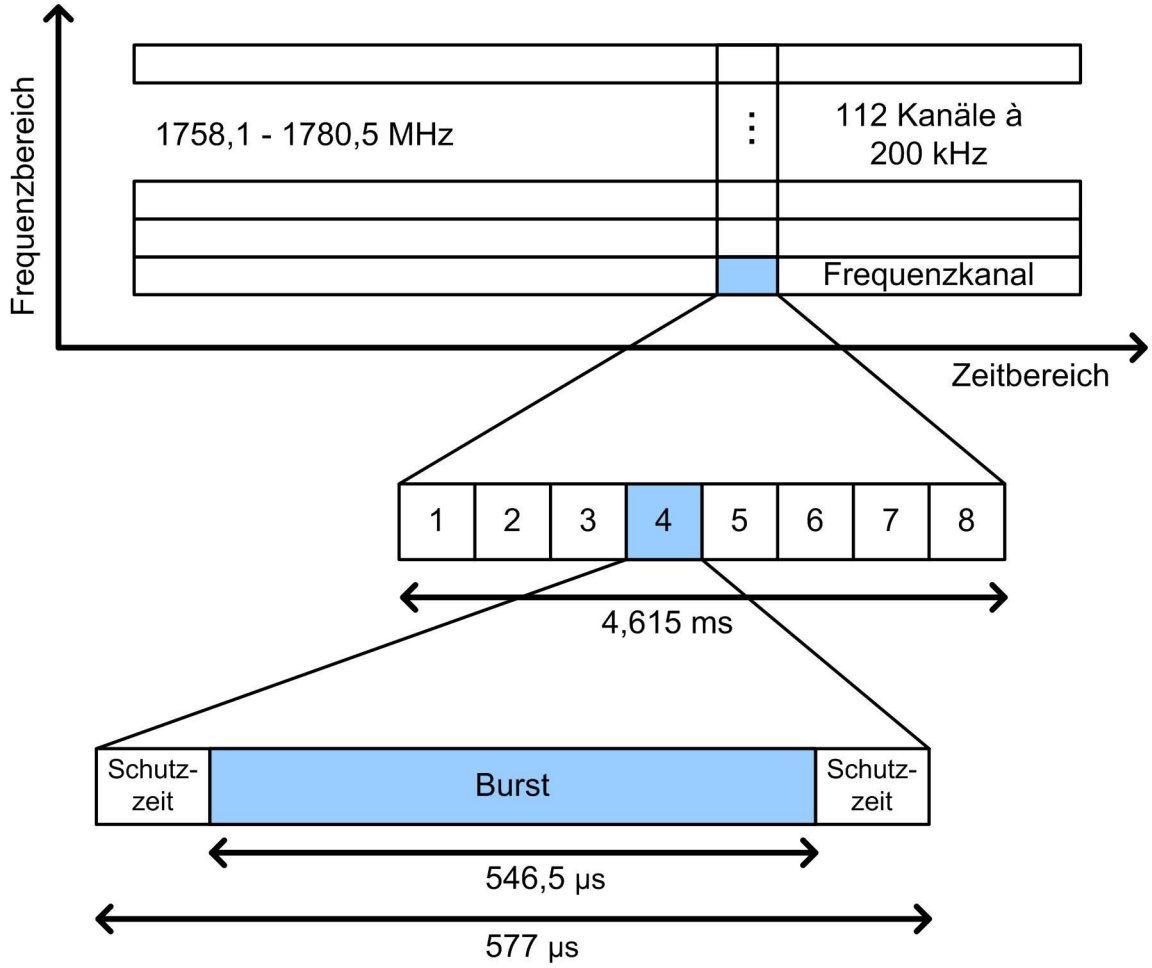
Bei GSM sind für den Uplink – also die Verbindung vom Mobiltelefon zum Netz – und den Downlink unterschiedliche Übertragungsfrequenzen vorgesehen. Das Endgerät wechselt dabei in Intervallen zwischen den Frequenzbereichen für Versand und Empfang, wodurch eine gemeinsame Antenne genutzt werden kann. Dabei werden die folgenden Frequenzbereiche verwendet:

Tabelle 1: Für die Nutzung durch GSM reservierte Frequenzbänder

Frequenz-bereich	Uplink	Downlink	Kontinent	Anmerkungen
450 MHz	450,4 bis 457,6 MHz	460,4 bis 467,6 MHz	für GSM nur selten eingesetzt	Wird in den Spezifikationen der 3GPP auch als GSM 400 bezeichnet.
480 MHz	478,8 bis 486 MHz	488,8 bis 496 MHz	für GSM nur selten eingesetzt	Wird in den offiziellen Spezifikationen der 3GPP auch als GSM 400 bezeichnet.
750 MHz	747,0 bis 762,0 MHz	777,0 bis 792,0 MHz	für GSM bisher nicht eingesetzt	Wird als GSM 750 oder missverständlich als GSM 700 bezeichnet.
850 MHz	824,0 bis 849,0 MHz	869,0 bis 894,0 MHz	Amerika	Wird als GSM 850 oder missverständlich als GSM 800 bezeichnet.
900 MHz	876,0 bis 880,0 MHz	921,0 bis 925,0 MHz	Asien, Europa	Wird als GSM-R bezeichnet; reserviert für Eisenbahngesellschaften.
900 MHz	880,0 bis 890,0 MHz	925,0 bis 935,0 MHz	Europa	Wird als E-GSM-Band (Extended GSM) bezeichnet, da nachträglich das Frequenzband um 10 MHz erweitert wurde. Allgemeine Bezeichnung: GSM 900
900 MHz	890,0 bis 915,0 MHz	935,0 bis 960,0 MHz	Afrika, Amerika, Asien, Australien, Europa	Wird als P-GSM-Band (Primary GSM) bezeichnet, da ursprünglich nur 890,0 MHz bis 915,0 MHz und 935,0 MHz bis 960,0 MHz vorgesehen waren. Allgemeine Bezeichnung: GSM 900
1800 MHz	1710,0 bis 1785,0 MHz	1805,0 bis 1880,0 MHz	Afrika, Amerika, Asien, Australien, Europa	Wird als GSM 1800 bezeichnet.
1900 MHz	1850,0 bis 1910,0 MHz	1930,0 bis 1990,0 MHz	Amerika	Wird als GSM 1900 bezeichnet.

Die Verfügbarkeit der Frequenzbänder für GSM variiert, wie aus Tabelle 1 ersichtlich, erheblich von Kontinent zu Kontinent. Aber auch auf nationaler Ebene findet man eine starke Zersplitterung der freigegebenen Frequenzbänder vor. Die Differenzen in den eingesetzten Frequenzen führten dazu, dass internationale Reisende in der Regel auf Dual-, Tri- oder sogar Quad-Band-Endgeräte angewiesen sind, um einen weltweiten Zugriff auf GSM-Netze zu erreichen. In Deutschland sind die Bereiche 890 bis 915 MHz, 935 bis 960 MHz, 1725 bis 1780 MHz und 1820 bis 1875 MHz für die Nutzung durch GSM freigegeben. Ende 2005 wurden diese Bänder um die Bereiche 880 bis 890 MHz sowie 925 bis 935 MHz erweitert, sodass nun nahezu dieselben Frequenzbänder wie beispielsweise in den Nachbarstaaten Österreich und Schweiz freigegeben sind. Innerhalb dieser Frequenzbänder werden Teilbereiche auf nationaler Ebene an kommerzielle Netzbetreiber lizenziert (z. B. die Bereiche 1758,1 bis 1780,5 MHz und 1853,1 bis 1875,5 MHz).

Abbildung 2: Frequenz- und Zeitmultiplexing unter GSM (eine Senderichtung)



Bei GSM handelt es sich um ein digitales Funknetz. Die dem Netzbetreiber zur Verfügung gestellten Frequenzbänder werden nach dem Frequency Division Multiplexing Access Verfahren (FDMA) in Kanäle unterteilt. Jeder Kanal belegt eine Bandbreite von 200 kHz und wird auf eine entsprechende Trägerfrequenz aufmoduliert (z. B. 1758,2 MHz als Mittenfrequenz bei einem Kanal von 1758,1 bis 1758,3 MHz). Das FDMA-Verfahren mit statischen Kanälen reicht aber bei Weitem nicht aus, um innerhalb des Empfangsbereichs einer Mobilfunkzelle (BTS) alle Endgeräte mit dem GSM-Dienst zu versorgen. Die statische Reservierung von Kanälen alleine führt zu einer schlechten Ausnutzung der durch den Funkraum zur

Verfügung gestellten Gesamtbandbreite. Daher kommt innerhalb der Frequenz-Kanäle eine weitere Unterteilung auf Basis von Zeitschlitzen (kurze Zeitabschnitte, englisch time slots) zum Einsatz.

Diese Time Division Multiplex Access (TDMA) genannte Technik kommt in ähnlicher Form in Festnetzen zum Einsatz, z. B. bei Integrated Services Digital Network (ISDN). TDMA unterteilt zur Realisierung weiterer Kanäle den Frequenzkanal in der Zeitachse in sogenannte Rahmen. Diese Rahmen haben eine Dauer von 4,615 ms und umfassen acht Zeitschlitze mit einer Länge von je 15/26 ms (ca. 0,577 ms). Jeder dieser Zeitschlitze steht nun für die Übertragung eines GSM-Kanals zur Verfügung, d. h. jedem Sender steht alle 4,615 ms ein Zeitfenster von 0,577 ms für die Datenübertragung zur Verfügung. Jeder Zeitschlitz ist umgeben von zwei Schutzzeiträumen von rund 15 µs Dauer, die einer versehentlichen Überlagerung entgegenwirken sollen. Zwischen diesen ist ein sogenannter Burst (Folge von Symbolen) aus digitalen Daten enthalten.

Beim Einsatz von TDMA in Funknetzen ergibt sich ein technisches Problem. In einem Festnetz ist die Entfernung von Sender und Empfänger nicht variabel und alle Sender und Empfänger, die sich desselben Kabels bedienen, sind gleich weit voneinander entfernt. Das trifft in einem Mobilfunknetz in aller Regel nicht zu, was problematische Auswirkungen auf das sensible Timing von TDMA hat. Da sich elektromagnetische Signale zwar mit sehr hoher, aber dennoch endlicher Geschwindigkeit ausbreiten (die sogenannte Gruppengeschwindigkeit), kommt es bei großen Entfernungen zwischen Sender und Empfänger zu technisch relevanten Signalverzögerungen. Das kann dazu führen, dass ein gesendeter Burst erst nach Ablauf des ihm vom Empfänger zugewiesenen Zeitfensters eintrifft. Da andere Zeitfenster auf derselben Frequenz von weiteren Mobilfunkteilnehmern genutzt werden, kommt es mit großer Wahrscheinlichkeit zu Überschneidungen. Um diesem Problem zu begegnen, sieht der GSM-Standard den Timing Advance Mechanismus vor. Sobald der Empfänger eine Überschreitung des Zeitfensters feststellt, wird dem Sender der gleichnamige Parameter übermittelt. Dieser gibt in 64 diskreten Schritten à 3,7 µs den ungefähren Laufzeitunterschied zwischen den Netzteilnehmern an. Ein Wert von 1 veranlasst den Sender also, den Burst 3,7 µs vor Beginn des ihm zugewiesenen Zeitfensters zu versenden. 3,7 µs entsprechen einer Entfernung des Senders von 553 Meter, wobei die Laufzeiten des Hin- und Rückweges beachtet wurden. Diese relativ grobe Korrektur des Timings ermöglicht maximale Entfernungen von immerhin 35 Kilometern zwischen Sender und Empfänger. Dass keine Zwischenwerte abgebildet werden können, wird durch entsprechende Schutzzeiten zwischen den Bursts ausgeglichen.

Die digitalen Daten werden per Gaussian Minimum Shift Keying (GMSK) auf das elektromagnetische Trägersignal aufmoduliert. Dieses Modulationsverfahren ist die digitale Form der Frequenzmodulation, es variiert also die Frequenz und nicht die Amplitude des Trägersignals. Jede Frequenz des Signals steht hierbei für einen zu codierenden Wert. Der Abstand zwischen diesen diskreten Frequenzen wird als Frequenzhub bezeichnet. Das Verhältnis von Frequenzhub zu der Frequenz des zu codierenden Signals (respektive der Bitrate bei digitalen Signalen) wird als Modulationsindex bezeichnet. Frequenzhub und Modulationsindex sind die charakteristischen Parameter eines Frequenzmodulationsverfahrens. Das GMSK hat einen Modulationsindex von $\eta=0,5$, was als Minimum Shift Keying bezeichnet wird. Ein zu codierender Bitstrom hat die Form eines Rechtecksignals. Die in einem solchen Signal enthaltenen Amplitudensprünge haben theoretisch ein unendliches Frequenzspektrum, weshalb ihre Modulation eine theoretisch unendlich hohe Bandbreite des Trägersignals voraussetzt. Daher wird für eine bandbreiteneffiziente Modulation im Unterschied zur herkömmlichen binären Phasenmodulation (Binary Phase Key Shifting, BPSK) beim GMSK das zu codierende

Rechtecksignal anhand eines gaußschen Filters umgeformt. Die Rechtecksfolge wird zu einer Folge von Gauß-Glocken „geglättet“, wodurch die für die Codierung irrelevanten Frequenzanteile entfallen. Als Folge wird jedoch die Impulsdauer erheblich verlängert (ungefähr um den Faktor fünf), was zu einer starken Überlagerung einzelner Impulse führt. Diese werden auf Empfängerseite durch Filter aus dem Signal entfernt.

Die Länge eines Bursts liegt, abzüglich der Schutzzeiten, bei rund 546 µs. Danach können mit dem verwendeten Modulationsverfahren rein rechnerisch ca. 156 Bit übertragen werden. Somit ergibt sich eine Rohdatenrate von ca. 270,1 kbit/s, also rund 33,9 kbit/s für jeden der acht Zeitkanäle. Für die die Nutzdaten umgebenden Rahmenstrukturen werden hiervon weitere 9,2 kbit/s abgezogen. Durch die benötigten Steuerkanäle sowie die Korrektur der auf der Luftschnittstelle auftretenden Fehler halbiert sich der Restwert nahezu, woraus eine Nettodatenrate von rund 13 kbit/s resultiert. Auf dem gesamten Frequenzkanal entspricht dies also einer Bandbreite von 104 kbit/s. Durch den Einsatz schwächerer Fehlerkorrekturen lässt sich dieser Wert innerhalb gewisser Grenzen erhöhen. So könnten bei Abschaltung jeglicher Fehlerkorrektur maximal 22,8 kbit/s erreicht werden.

Die bisherige Betrachtung bezieht sich auf die unidirektionale Übertragung vom Sender zum Empfänger. Da es sich aber sowohl bei mobilen Endgeräten als auch bei BTS um Transceiver, also kombinierte Sender und Empfänger handelt, musste ein Verfahren zum (scheinbar) gleichzeitigen Empfang und Versand von Daten gefunden werden. Wie oben bereits erwähnt stehen für Versand und Empfang der Daten getrennte Frequenzbänder zur Verfügung. Damit nun nur eine Antenne im mobilen Endgerät zum Einsatz kommen muss, wird zwischen Sende- und Empfangsmodus abgewechselt. Der zeitliche Abstand zwischen Sende- und Empfangsmodus beträgt genau drei Zeitschlitze und es wird alle 2,31 ms umgeschaltet. Die Frequenzpaare können nach jedem Zyklus gewechselt werden, was dann 217 Kanalwechseln pro Sekunde entspricht. Dadurch verringert sich der Einfluss von Störungen auf einzelnen Frequenzkanälen.

Sobald der Besitzer sein Mobiltelefon einschaltet, sucht das Gerät ein geeignetes Empfangssignal. Dabei scannt es die zum GSM-Band gehörenden Frequenzen, z. B. bei GSM-900 173 Kanäle, nach einem Frequency Correction Burst (FCB) ab. Dieser Burst legt die Frequenz fest, auf der das Mobiltelefon nun auf einen Synchronisation Burst wartet. Dieser ermöglicht das Mobiltelefon mit dem GSM-Netz zeitlich zu synchronisieren. Nach erfolgter Frequenz- und Zeitsynchronisation können nun über den Broadcast Control Channel (BCCH) Daten empfangen werden, die Informationen über das Netz enthalten. Derartige Informationen sind zum Beispiel der Mobile Country Code (MCC), der Mobile Network Code (MNC) sowie der Local Area Code (LAC) und der Cell Identifier (CI), die zusammen Netz und Zelle eindeutig kennzeichnen. Wenn diese Zelle genutzt werden darf und das Signal genügend stark ist, d. h. die Pegelbedingungen erfüllt sind, versucht sich das Mobiltelefon im Netz anzumelden. Andernfalls wird versucht, zu einer anderen Zelle eine Verbindung aufzubauen.

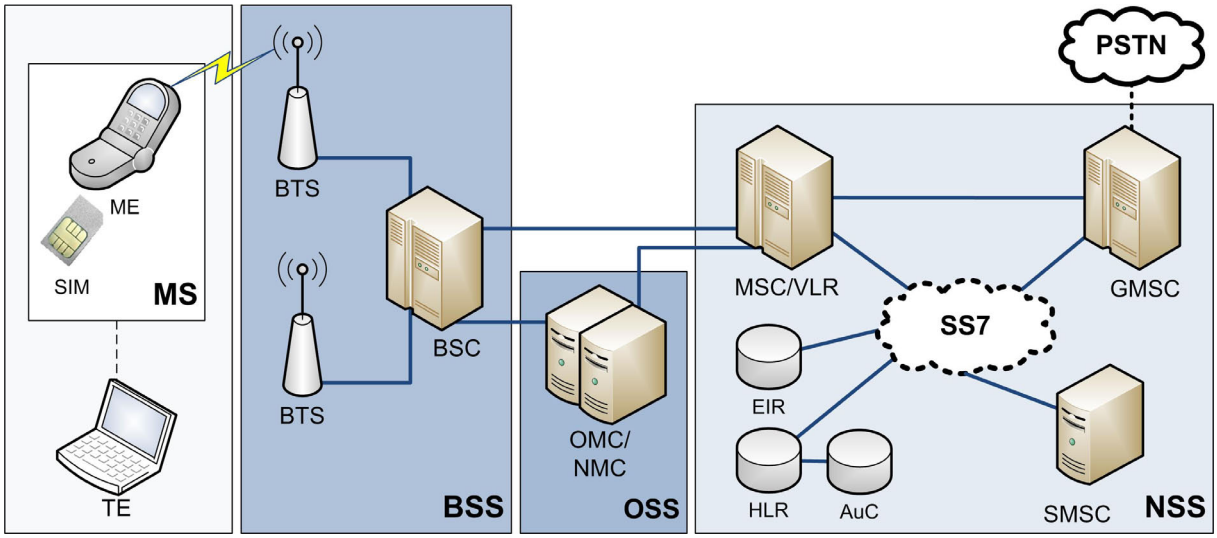
Die Anmeldung im Netz erfolgt auch, wenn kein Gespräch geführt werden soll. Das Mobiltelefon fordert vom BSC einen Funkkanal an, indem es einen Random Access Burst in einem vorgesehenen Zeitschlitz schickt. Der Random Access Burst füllt das Zeitfenster jedoch nicht völlig aus, um eventuelle laufzeitbedingte Überschneidungen zu vermeiden. Eine etwaige Zeitverschiebung wird von der BTS benutzt, um den Timing Advance Parameter zu bestimmen und so die Einhaltung der Zeitfenster zu gewährleisten. Danach erfolgt die Authentisierung (siehe Kapitel 1.2.1). Hierbei werden Daten zur Identität des Nutzers (IMSI) sowie die Seriennummer des Mobiltelefons (IMEI) und die Kennung der Basisstation, über

die die Anmeldung erfolgt ist, protokolliert und gespeichert. Weiterhin wird jeder Verbindungsversuch, unabhängig vom Zustandekommen der Verbindung, gespeichert.

1.1.3 Integrierte Dienste

Ein Dienst, der heutzutage untrennbar mit dem Mobiltelefon verbunden scheint, ist der Short Message Service, besser auch bekannt als SMS. Über diesen Dienst lassen sich Textnachrichten mit bis zu 160 Zeichen versenden. Realisiert wird dieser Telekommunikationsdienst mithilfe einer Kurzmitteilungszentrale (SMS Center, kurz SMSC), über die alle Nachrichten versendet werden. Diese Zentrale ist, wie in Abbildung 3 zu sehen, in das SS7-Netz integriert und gehört somit zum NSS. Die SMSC baut über den MSC Verbindungen zu mobilen Endgeräten auf oder kann über den GMSC Verbindungen zu anderen Mobilfunk-Anbietern aufbauen, falls der Empfänger sich nicht im eigenen GSM-Netz befinden sollte.

Abbildung 3: Lokalisierung des SMS Center im GSM-Netz



Ähnlich wie der Kurznachrichtendienst ist der EMS (Enhanced Messaging Service) sowie der MMS (Multimedia Messaging Service) in das Mobilfunknetz eingebunden (siehe Kapitel 7 und Kapitel 9).

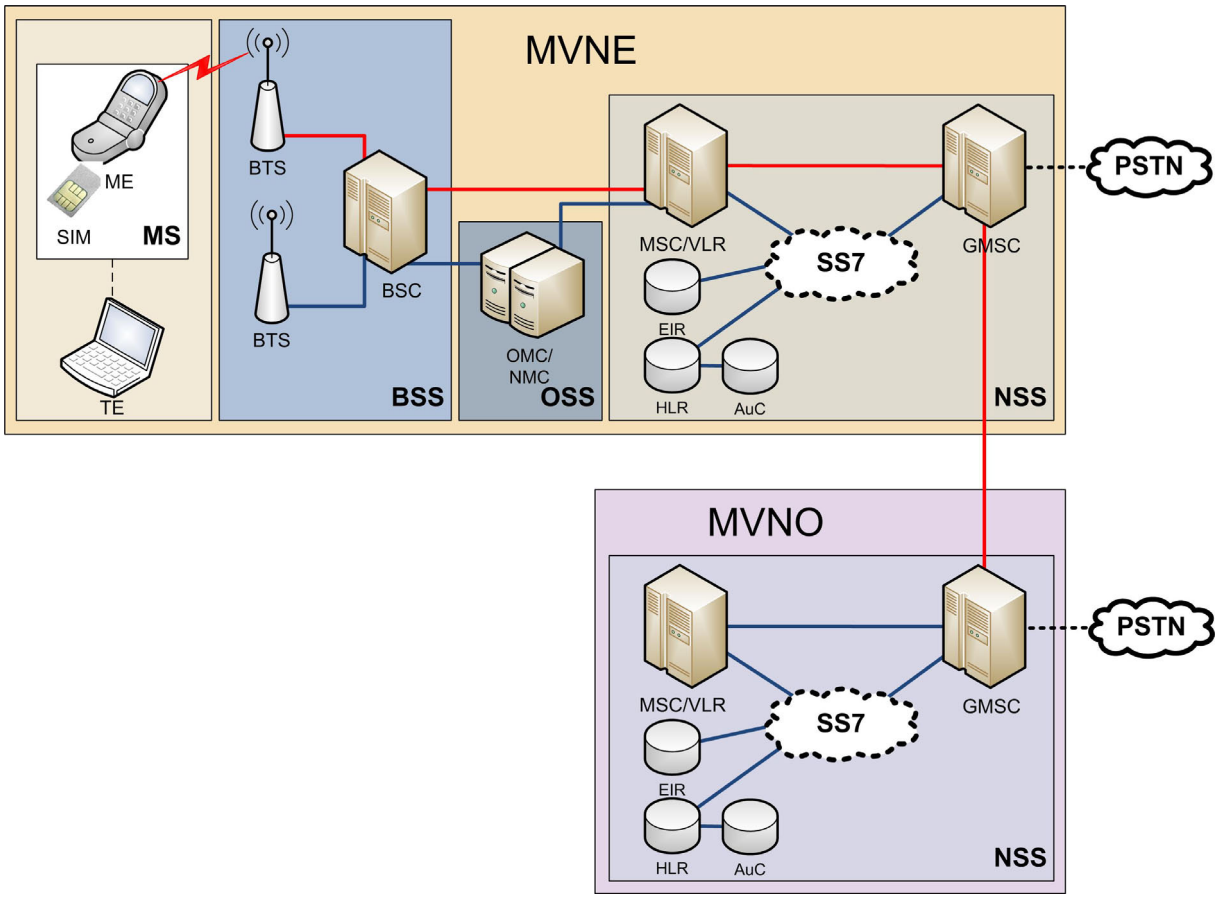
Die Integration solcher Nachrichtendienste eröffnet die Möglichkeit, Mehrwertdienste auf Basis von Kurznachrichten anzubieten, wie zum Beispiel Nachrichtenservices, Sportmeldungen oder aber auch die Zusendung von Informationen über die Region, in der sich das Mobiltelefon gerade befindet (siehe auch Kapitel 13). Die Einbindung der Mehrwertdienste in die Menüstruktur des Mobiltelefons kann über das sogenannte SIM Toolkit erfolgen. Dies erfordert eine spezielle SIM-Karte in Kombination mit einem Mobiltelefon, die beide den Standard SIM Toolkit unterstützen müssen (auch „SAT SIM Application Toolkit“ genannt, siehe [3GPP22038]). Dadurch können im laufenden Betrieb Daten und Programme per SMS in den SIM-Karten-Speicher geladen und so das Mobiltelefon neu programmiert werden, um den Zugriff zum Beispiel auf neue Serviceangebote zu ermöglichen. Solche Funktionen müssen autorisierten Stellen vorbehalten bleiben, da sie ein potenzielles Sicherheitsrisiko für den Endanwender darstellen (siehe dazu Kapitel 16).

1.1.4 Integrierte Dienstanbieter

Auf dem Markt gibt es Unternehmen, im Allgemeinen auch Mobilfunkdiscounter genannt, die wie Mobilfunkbetreiber auftreten, jedoch weder über die benötigten Sendelizenzen verfügen noch die erforderliche Infrastruktur besitzen, um ein Netzbetreiber (Mobile Network Operator, MNO) zu sein. Vielmehr mieten diese Mobile Virtual Network Operator (MVNO) Kapazitäten von vorhandenen Mobilfunknetzbetreibern, welche in der Rolle des Mobile Virtual Network Enabler (MVNE) die Mobilfunkvermittlungsstellen unterhalten und sich um die Netzverwaltung kümmern.

Wie sich ein MVNO in das bestehende Netz eines MVNEs eingliedert, ist nicht festgelegt und kann von Fall zu Fall unterschiedlich sein. Hierbei ist entscheidend, inwieweit sich der MVNO vom MVNE lösen möchte bzw. es ihm der MVNE ermöglicht, die Dienste anzubieten, die er seinen Kunden offerieren möchte. Größtmögliche Flexibilität und Freiheitsgrade bietet eine fast unabhängige Struktur, wie in Abbildung 4 dargestellt. Der MVNO besitzt ein bis auf das BSS und OSS eigenständiges Netz. Dies bedeutet, dass insbesondere die Kundendatenverwaltung, die Authentisierung und das Herstellen von Verbindungen in den Aufgabenbereich des MVNOs fallen. Der MVNE leitet Authentisierungs-, Verbindungs- und weitere Dienstanfragen ausgehend von Mobiltelefonen des MVNO-Kunden an dessen (G)MSC weiter, der dann entsprechend agiert.

Abbildung 4: Integration virtueller Mobilfunk-Anbieter



Das andere Extrem ist die völlige Virtualisierung eines Mobilfunk-Anbieters. Hierbei werden sämtliche Ressourcen vom MVNE gestellt.

Ein virtueller Mobilfunk-Anbieter (MVNO) kann seine Dienstleistungen auch auf mehrere MVNEs verteilen und so zum Beispiel über Ländergrenzen hinweg sein Netz ausbauen. Bei Anbindung von mehreren MVNEs bezeichnet man den Anbieter auch als roaming Mobile Virtual Network Operator (rMVNO).

1.2 Sicherheitsfunktionen

Im Folgenden werden die gängigen Sicherheitsfunktionen innerhalb eines GSM-Netzes beschrieben. Dies betrifft die Bereiche Authentifizierung, Verschlüsselung sowie Schutz der Privatsphäre. Hierbei wird bereits auf denkbare Sicherheitsgefährdungen im jeweiligen Kontext verwiesen. Eine Auflistung tatsächlicher Sicherheitsgefährdungen erfolgt anschließend im Kapitel 1.3.

1.2.1 Authentisierung

Ein wesentlicher Sicherheitsfaktor innerhalb des GSM-Netzes ist die Überprüfung der Identität eines Funknetzteilnehmers durch den Funknetzbetreiber. Der Schlüssel zur Identitätsverwaltung des Teilnehmers ist die auf der SIM-Karte gespeicherte und weltweit eindeutige IMSI. Über diesen Schlüssel können alle zugehörigen Identitätsinformationen inklusive dem Shared Secret eindeutig referenziert werden.

Bevor eine SIM-Karte an den Kunden eines Mobilfunk-Anbieters ausgeliefert wird, erfolgt zunächst eine Personalisierung. Im Verlauf dieses Vorgangs wird die SIM-Karte für den entsprechenden Kunden parametrisiert. Hierzu gehören unter anderem:

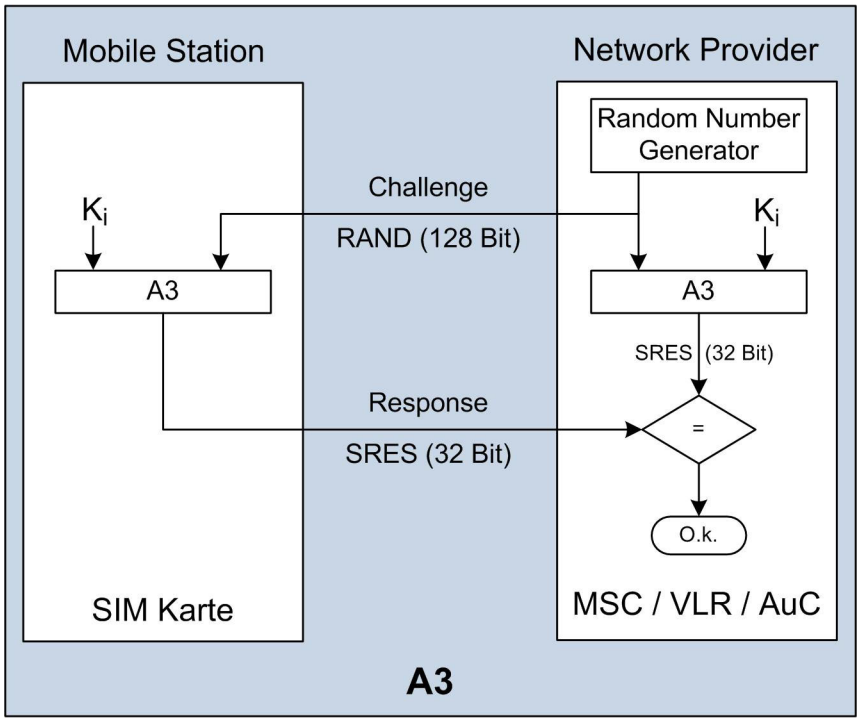
- Die Generierung und Speicherung eines Subscriber Authentication Key (Shared Secret, K_i in Abbildung 5) sowohl auf der Karte als auch in der Benutzerdatenbank des Mobilfunk-Anbieters

- Die Zuordnung einer Rufnummer zur IMSI der SIM-Karte

Die Personal Identification Number (PIN), die zunächst vom Mobilfunk-Anbieter festgelegt wird, kann später vom Benutzer der SIM-Karte geändert werden und dient zur Authentisierung des Benutzers gegenüber der SIM-Karte, um eine missbräuchliche Verwendung zu verhindern. Nach drei falschen Eingaben der PIN wird die SIM-Karte gesperrt. Eine gesperrte SIM-Karte kann über den zugehörigen Personal Unblocking Key (PUK) wieder freigeschaltet werden. Nach zehn falschen PUK-Eingaben wird die SIM-Karte unwiederbringlich gesperrt und muss ausgetauscht werden. Ebenso wie die PIN wird der PUK vom Mobilfunk-Anbieter generiert und auf der SIM-Karte gespeichert. Jedoch kann der PUK nicht vom Benutzer geändert werden.

Der 128 Bit lange Subscriber Authentication Key wird bei der Aufnahme eines neuen Benutzers in ein Mobilfunknetz vom Mobilfunk-Provider generiert. Er wird sowohl in der SIM-Karte als auch im Nutzerverzeichnis (HLR) gespeichert, weshalb man ihn auch als Shared Secret bezeichnet. Der Subscriber Authentication Key kann im Nachhinein weder ausgelesen noch geändert werden. Er wird ausschließlich mittels eines auf der SIM-Karte gespeicherten Algorithmus für die digitale Signatur im Rahmen eines Challenge-Response-Verfahrens und zur Berechnung eines Sitzungsschlüssels zur Datenverschlüsselung verwendet (siehe Kapitel 1.2.2).

Abbildung 5: Einseitige Authentisierung mittels A3-Algorithmus



Im ersten Schritt zur Authentisierung der Mobilen Station (MS) am BSS/NSS übermittelt die MS die auf der SIM-Karte hinterlegte IMSI an das HLR. Diese Übertragung geschieht unverschlüsselt. Über die IMSI wird der im HLR gespeicherte Subscriber Authentication Key (K_i in Abbildung 5) referenziert und dem AuC zur Verfügung gestellt. Das AuC generiert eine Challenge (128 Bit lange Zufallszahl) und sendet diese zurück an die MS. Unter Verwendung des A3-Algorithmus wird hierzu sowohl vom Endgerät (SIM-Karte) als auch vom AuC der Authentisierungs-Schlüssel (32 Bit Signed Response) berechnet. Wenn die getrennt berechneten Responses übereinstimmen, ist der Teilnehmer authentisiert.

Wichtig hierbei ist, dass keine Authentisierung der BSS gegenüber dem Endgerät erfolgt. Diese einseitige Vertrauensstellung der BSS stellt eine massive Sicherheitslücke dar und kann für Angriffe ausgenutzt werden (vergleiche IMSI-Catcher in Kapitel 1.3.1).

Der zur Erzeugung des Authentisierungs-Schlüssels verwendete A3-Algorithmus ist nicht in GSM standardisiert. Es gibt im GSM-Standard zwar Beispielimplementierungen, allerdings ist der Netzbetreiber frei in der Wahl einer „geeigneten“ Implementierung. Die Korrektheit der Implementierung ist somit nicht gewährleistet, woraus sich eine potenzielle Sicherheitsgefährdung ergibt.

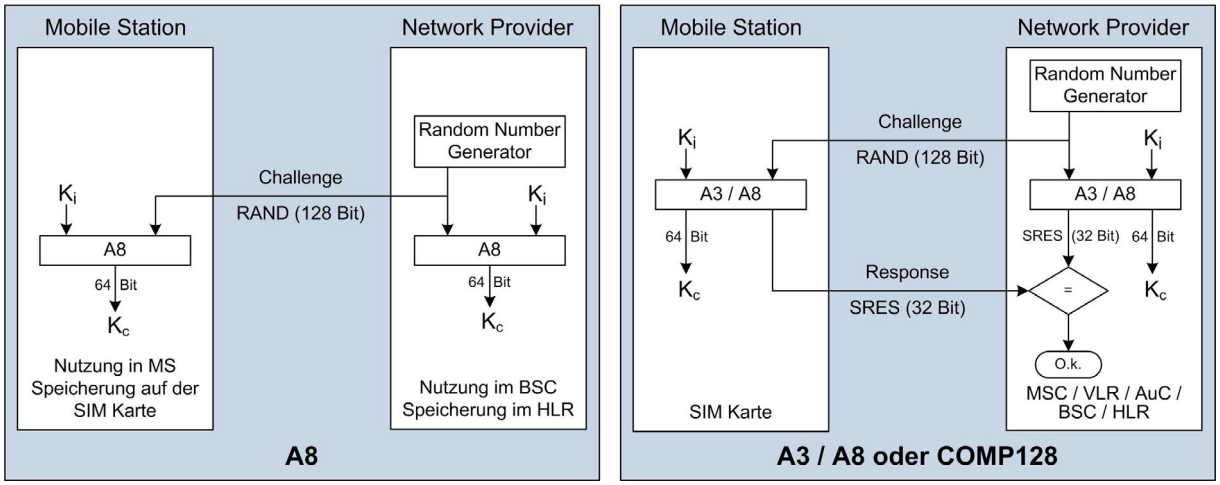
Anmerkung: Auch Beispielimplementierungen können fehlerhaft sein. So ließen sich zum Beispiel in den 1990er Jahren vorübergehend SIM-Karten eines großen Mobilfunkbetreibers erfolgreich klonen, obwohl dieser sich an die damals aktuelle Beispielimplementierung gehalten hatte.

1.2.2 Verschlüsselung

Aus dem Subscriber Authentication Key (K_i) und der während der Authentisierung erstellten Challenge (128 Bit Zufallszahl) wird unter Verwendung des A8-Algorithmus sowohl vom

Endgerät (SIM-Karte) als auch vom AuC ein Session Key (64 Bit) berechnet. Der A8-Algorithmus ist ebenso wie A3 nicht in GSM standardisiert. Zwar gibt es auch hierfür Beispielimplementierungen, allerdings ist der Netzbetreiber frei in der Wahl einer „geeigneten" Implementierung. Auch hier ergibt sich aus der Implementierungsfreiheit eine potenzielle Sicherheitsgefährdung.

Abbildung 6: Kombination von A3 und A8 - erleichterte Angriffe auf die Verschlüsselung



Der mithilfe des A8-Algorithmus erzeugte 64 Bit Session Key (wobei nur 56 Bit variabel sind, 8 Bit sind fest) wird für die Verschlüsselung der Daten über die Luftschnittstelle zwischen MS und BTS eingesetzt. Der Algorithmus zur Verschlüsselung heißt A5. Man unterscheidet vier Varianten des A5-Standards.

- A5/0: Dieser wurde nachträglich in den Standard aufgenommen und enthält keine Verschlüsselung.

- A5/1: Bei A5/1 handelt es sich um einen Stromchiffre. Der zugrunde liegende Algorithmus wurde geheim gehalten, jedoch über Reverse Engineering nachgestellt. Mittlerweile sind vielfältige Angriffsmöglichkeiten bekannt.

- A5/2: A5/2 ist wie A5/1 ein Stromchiffre. Es handelt sich um eine abgeschwächte Version des A5/1, der extrem anfällig für Angriffe ist. Seit 2006 fordert die GSM Association, dass mobile Geräte diesen Algorithmus nicht länger unterstützen. Der Algorithmus wurde ebenfalls geheim gehalten, jedoch über Reverse Engineering nachgestellt. Auch hierfür sind viele Angriffsmöglichkeiten bekannt.

- A5/3: Dieser ist auch als MISTY bekannt und identisch mit dem in UMTS-Netzen verwendeten KASUMI-Algorithmus (japanisch verschleiert). Es handelt sich im Gegensatz zu A5/1 und A5/2 um einen Blockchiffre. Die Spezifikationen dieses Algorithmus wurden von Beginn an offen gelegt (siehe [3GPP]), was die Erforschung und Schließung von Sicherheitslücken vereinfachte A5/3 wird bis heute als praktisch sicher (genug) angesehen, obwohl die ursprünglichen Beweisführungen hinsichtlich seiner Sicherheit bereits im Jahr 2005 widerlegt werden konnten und entsprechend neu formuliert werden mussten.

Es ist jedoch zu bemerken, dass nicht alle Daten der Luftschnittstelle verschlüsselt werden. Beispielsweise wird ein Cell Broadcast nie verschlüsselt, da hier alle in einer Funkzelle be-

findlichen Endgeräte die Meldungen mitlesen müssen. Eine Verschlüsselung würde hier keinen Sinn machen.

1.2.3 Schutz der Privatsphäre

Beim Verbindungsaufbau wird die IMSI unverschlüsselt übertragen (notwendig, da das AuC anhand der IMSI den Subscriber Authentication Key, welcher für die Berechnung des Crypto-Schlüssels benötigt wird, im HLR referenziert).

Anschließend wird zur Identifizierung des Teilnehmers eine zufällig generierte Temporary Mobile Subscriber Identity (TMSI) vergeben, welche regelmäßig gewechselt wird. Ein Wechsel der TMSI wird

- bei Wechsel der Funkzelle und
- in regelmäßigen Zeitabständen

vorgenommen. Das Verwenden einer ständig wechselnden, zufälligen TMSI dient dem Schutz der Privatsphäre der Teilnehmer, da somit

- das Erstellen von Bewegungsprofilen und
- das Erstellen von Kommunikationsprofilen (Gesprächspartner, in Anspruch genommene Dienste usw.)

auf Basis einer bekannten IMSI durch Abhören des Funkverkehrs nicht möglich ist.

Hierbei ist jedoch anzumerken, dass das Erstellen von Bewegungsprofilen auch mithilfe von Mobiltelefon-Ortungen möglich ist. Hierbei ist die Kenntnis der aktuellen TMSI nicht notwendig, da die Ortung über die Rufnummer des Mobiltelefons erfolgt (siehe Kapitel 13.1.1).

1.3 Sicherheitsgefährdungen

Im Folgenden werden Sicherheitsgefährdungen beschrieben, die zum einen aus der GSM Systemarchitektur herrühren und zum anderen die Datenerfassung betreffen.

1.3.1 Systemarchitektur

Die Netzbetreiber sind frei in der Wahl der Implementierung des A3- und A8-Algorithmus. Dies stellt eine potenzielle Sicherheitsgefährdung dar und erfordert ein hinreichendes Vertrauen zu dem jeweiligen Netzbetreiber.

In GSM-Netzen muss sich das mobile Endgerät gegenüber der BTS authentisieren – nicht aber umgekehrt. Dies ermöglicht Man-in-the-Middle-Angriffe unter Verwendung sogenannter IMSI-Catcher. Hierbei kann der Angreifer gegenüber dem Endgerät eine BTS simulieren, während er selber sich mit dem Mobilfunkbetreiber verbindet und somit als Gateway für sämtliche nachfolgende Kommunikation fungiert. Anschließend kann der Angreifer das mobile Endgerät dazu veranlassen, den A5-Algorithmus A5/0 zu verwenden und somit die nachfolgende Kommunikation komplett unverschlüsselt zu übertragen. Es ist jedoch für den An-

greifer nicht unbedingt notwendig, die Verschlüsselung zu deaktivieren, da es ebenfalls dokumentierte Angriffsmethoden gibt (siehe [Rue07]), in denen bereits nach einer Vorlaufzeit von wenigen Sekunden die nachfolgende Kommunikation in Echtzeit entschlüsselt werden kann.

In den 1999 im Zuge der 3GPP-Initiative aktualisierten GSM-Spezifikationen wurde die Abhörbarkeit durch staatliche Einrichtungen (englisch lawful interception) als feste Anforderung definiert.

- „It shall be possible for law enforcement agencies to monitor and intercept every call and call attempt, and other service or call related user actions, in accordance with national laws. This shall apply to devices and/or via interfaces placed by the serving networks or home environments at the disposal of the national law enforcement agencies according to national law, and intended solely for lawful interception purposes."[1] (siehe [3GPP21133])

- Technische Details siehe [3GPP33107]

Bei Zugriff auf die hierfür implementierten technischen Einrichtungen durch Unbefugte kann Missbrauch betrieben werden. Es sind bereits Beispiele für einen entsprechenden Missbrauch durch Innentäter im Bereich von Mobilfunkbetreibern dokumentiert (siehe [FWA08]).

Auch ein nicht gesetzlich autorisiertes Abhören von Mobilfunkgesprächen (bzw. das Mitschneiden übertragener Daten) ist möglich. Als denkbarer Angriffspunkt ist hier zunächst ein BSS zu nennen, da innerhalb eines BSS oft Richtfunkübertragung genutzt wird. Diese kann unverschlüsselt erfolgen, selbst wenn zwischen mobilem Endgerät und BTS mittels A5 verschlüsselt wird. Somit kann bei Zugriff auf diese Richtfunkstrecke die Kommunikation abgehört werden. Dies gilt natürlich entsprechend auch bei physikalischem Zugriff auf andere Teile des Vermittlungsnetzes. Es bieten sich insbesondere Angriffspunkte für Innentäter im Bereich des Mobilfunkbetreibers. In den nachfolgenden Gefährdungen wird aus technischer Sicht gezeigt, welche Möglichkeiten des Missbrauchs existieren. Möglich sind beispielsweise Manipulationen an Switching-Komponenten per Fernwartung, wodurch Gespräche für ausgewählte Mobilfunkteilnehmer von diesen unbemerkt auch an zusätzliche ausgewählte Endgeräte übertragen werden. Ebenso sind sämtliche bekannten Angriffsmöglichkeiten auf kabelgebundene Netze innerhalb des Providerbackbone gegeben.

Nicht nur die aktuell übertragenen Daten können Ziel eines Innentäters sein. Auch das Benutzerprofil, welches aus persönlichen Daten, genutzten Services, Verbindungsdaten und Kommunikationspartnern samt den daraus ableitbaren Vorlieben über Kommunikationskanäle und Kommunikationsorten besteht, kann von einem Innentäter zusammengetragen werden.

[1] „Es muss für Strafverfolgungsbehörden möglich sein, jeden Anruf, Anrufversuch, Dienst und jede anrufbezogene Anwenderhandlung in Übereinstimmung mit der nationalen Gesetzeslage zu überwachen und zu unterbrechen. Dies muss auf Anordnung der Strafverfolgungsbehörden und in Übereinstimmung mit nationalem Recht auf Endgeräte und/oder auf Schnittstellen des diensterbringenden Netzes oder der Heimumgebung angewendet werden und ist alleinig der gesetzmäßigen Überwachung (englisch Lawful Interception) vorbehalten."

1.3.2 Datenerfassung

Über den Abruf von Informationen, in welche Funkzelle ein mobiles Endgerät aktuell eingebucht ist, kann eine Ortung des mobilen Endgeräts erfolgen. Die Genauigkeit dieser Ortung hängt von der Dichte der Funkzellen am aktuellen Standort des mobilen Endgerätes ab. Weitere Informationen zu diesem Thema finden sich in Kapitel 13.1.1. Durch die Protokollierung der Einbuchvorgänge - IMSI und Funkzellen-Identifikation werden verknüpft - besteht die Möglichkeit, ein Bewegungsprofil des Mobilfunknutzers zu erstellen.

Ein anderes Beispiel ist die EU-Richtlinie 2006/24/EG zur Vorratsdatenspeicherung (siehe [BMJ07]). Danach müssen Telekommunikationsunternehmen ab dem 01.01.2009 Telekommunikationsverkehrsdaten ihrer Kunden bei erfolgreichen Gesprächen speichern. Für den Mobilfunk bedeutet dies, dass die Anschlussnummer und IMEI des Anrufers, die Anschlussnummer und ggf. IMEI des Angerufenen, das Datum, die Uhrzeit zu Gesprächsbeginn und -ende, sowie die Kennung der genutzten Funkzellen bei Gesprächsaufbau für mindestens sechs Monate, aber höchstens sieben Monate gespeichert werden. Entsprechend gilt dies auch für Übermittlungen von Kurz-, Multimedia oder ähnlichen Nachrichten, bei denen zusätzlich der Zeitpunkt des Versendens und des Empfangs festgehalten werden. Darüber hinaus werden IP-Adresse (Internet-Protokoll-Adresse), Beginn und Ende der Nutzung und die Anschlusskennung gespeichert, wenn Verbindungen ins Internet hergestellt werden. Aus diesen gespeicherten Daten lassen sich Benutzer- und Bewegungsprofile erstellen und soziale Netze rekonstruieren. Da die Telekommunikationsverkehrsdaten bei dem Telekommunikationsunternehmen gespeichert werden, können auch Innentäter Zugriff auf diese Daten erlangen.

1.3.3 Liste der Gefährdungen

Die im Folgenden benannten Gefährdungen sind teilweise System-immanent und können vom Mobilfunknutzer nicht beeinflusst werden. Entsprechend ergreifbare Schutzmaßnahmen vom Mobilfunkbetreiber und/oder vom Mobilfunknutzer sind referenziert.

G.1 Mögliche Schwachstelle in Endgeräte-Authentisierung

Netzbetreiber können eine „geeignete“ Implementierung des A3-Algorithmus selber wählen. Diese muss nicht offen gelegt werden.

Keine geeigneten Schutzmaßnahmen für den Nutzer möglich

G.2 Potenzielle Schwachstelle in der Datenverschlüsselung

Netzbetreiber können eine „geeignete“ Implementierung des A8-Algorithmus selber wählen. Diese muss nicht offen gelegt werden.

Keine geeigneten Schutzmaßnahmen für den Nutzer möglich

G.3 Unzureichende Verschlüsselungsstärke

Verschiedene Echtzeit- und Offline-Angriffe gegen A5/1 und A5/2 sind bereits veröffentlicht worden, z. B.:

- IMSI-Catcher und Ausschalten der Verschlüsselung (siehe [DuD26002])

  Schutzmaßnahmen siehe M.1, M.2, M.3

- IMSI-Catcher mit Kenntnis eines Sitzungsschlüssels (siehe [DuD26002])

  Schutzmaßnahmen siehe M.2, M.3

- Brechen der Verschlüsselung (als Beispiel siehe [BiDu33401], siehe M.2)

  Schutzmaßnahmen siehe M.1, M.2, M.3

G.4 SIM-Karten-Cloning

Aufgrund einer Schwäche im A3-Algorithmus zur Berechnung der Response während der Authentisierungs-Phase ist es für bestimmte SIM-Karten aus den 1990er Jahren möglich, den Subscriber Authentication Key zu ermitteln und somit die SIM-Karte zu klonen. Dies trifft jedoch nicht mehr auf SIM-Karten zu, welche ab 2001 zum Einsatz kommen.

Schutzmaßnahmen siehe M.5, M.6

G.5 Abhören von Telefonaten durch Zugriff auf Providernetz

Solche Fälle von Abhörangriffen durch Innentäter bei Mobilfunkbetreibern sind bereits dokumentiert.

Schutzmaßnahmen siehe M.2

G.6 Missbrauch von Standard-Leistungsmerkmalen

Die Leistungsmerkmale eines GSM-Netzes können auf vielfältige Weise missbraucht werden. Dies ermöglicht z. B. das Abhören von Raumgesprächen (siehe Kapitel 6).

Schutzmaßnahmen siehe M.4

G.7 Erstellung von Bewegungsprofilen durch Ortung

Eine detaillierte Beschreibung der Ortungsmöglichkeiten ist in Kapitel 13.1.1 enthalten.

Schutzmaßnahmen siehe M.3, M.4.

G.8 Unterbindung von Mobilfunkkommunikation

Mithilfe von Störsendern (englisch jammer) lässt sich sämtliche Kommunikation mit mobilen Endgeräten wirksam unterbinden. Das kommt einer Denial-of-Service-(DoS)-Attacke gleich. Der Einsatz von aktiven Störsendern ist in Deutschland zumeist verboten. In einigen Bundesländern ist mittlerweile der Einsatz z. B. in Gefängnissen erlaubt, jedoch nur unter strengen Rahmenbedingungen. De facto sind solche Geräte jedoch erwerbbar und kommen auch nachweislich immer wieder zum Einsatz.

Keine geeigneten Schutzmaßnahmen möglich

G.9 Software-Manipulation

Durch Software-Manipulation oder Modifikation der Software in den mobilen Geräten, lässt sich die Kommunikation auf viele Arten kompromittieren (Firmware, Programme, Viren usw., siehe Kapitel 16).

Schutzmaßnahmen siehe M.88 bis M.95

G.10 Mobiltelefon als Abhörgerät

Durch Manipulation der Endgeräte-Hardware und Software lässt sich ein Mobiltelefon als Abhöreinrichtung missbrauchen (Einbau von Abhöreinrichtungen, Akku mit integrierter Mobilstation usw., siehe Kapitel 14).

Schutzmaßnahmen siehe M.4

G.11 Vorratsdatenspeicherung

Die Erstellung von Benutzer- und Bewegungsprofilen sowie eine Rekonstruktion von sozialen Netzwerken auf Grundlage der Vorratsdatenspeicherung sind möglich.

Schutzmaßnahmen siehe M.1, M.10

G.12 Man-in-the-Middle-Attacke

IMSI-Catcher funktionieren in GSM-Netzen, da sich der Betreiber gegenüber dem Endgerät nicht authentisieren muss (kein gegenseitiges Challenge-Response Verfahren). Daher kann der in Kapitel 1.3.1 beschriebene IMSI-Catcher zum Einsatz kommen (siehe [MeWe04]).

Schutzmaßnahmen siehe M.1, M.2

1.4 Mögliche Schutzmaßnahmen

Die aufgeführten Schutzmaßnahmen erlauben es dem Mobilfunknutzer, Gefährdungen zu minimieren; lediglich die Maßnahmen M.11 und M.12 adressieren Dienstanbieter.

M.1 Sicherheitsanzeige

Verwendung von Mobiltelefonen mit Warnfunktion bei unverschlüsselter Verbindung (beispielsweise je nach Hersteller durch ein offenes Schloss-Symbol am oberen Bildschirmrand dargestellt)

M.2 (Sprach-)Datenverschlüsselung

Verwendung von vertrauenswürdigen Crypto-Mobiltelefonen, Crypto-Sprach-Ein-Ausgabemodulen (Hardware) oder Crypto-Software zum Aufbau einer Ende-zu-Ende-Verschlüsselung

M.3 Verschleierung der Identität gegenüber dem Mobilfunkbetreiber

Ein häufiges Wechseln des Mobiltelefons inklusive SIM-Karte hilft, die eigene Identität - zumindest temporär – gegenüber dem Dienstanbieter oder eventuellen Angreifern zu verschleiern. Es senkt die Gefahr, dass benutzerspezifische Daten wie etwa die IMSI einem Nutzer eindeutig zugeordnet werden können. Dieses Vorgehen wird erschwert, wenn zum Schutz vor Diebstahl das Endgerät auf die Verwendung mit einer einzigen SIM-Karte eingeschränkt wird (siehe M.7). Darüber hinaus besteht die Gefahr, dass bei Weitergabe von Endgeräten oder SIM-Karten, ob nun unter den Mitarbeitern eines Unternehmens oder sogar über Tauschbörsen, persönliche Daten in unbefugte Hände gelangen (siehe G.67). Hier muss also eine Abwägung getroffen werden, ob die Verschleierung der Nutzeridentität oder die Datensicherheit priorisiert wird.

M.4 Ausschalten des Mobiltelefons und ggf. Entnahme des Akkus

Da einfaches Drücken des Ausschalters bei einigen Geräten nicht den Mobilfunkteil deaktiviert, muss zur Sicherheit zusätzlich der Akku entfernt werden.

Ausnahme: Es gibt in Akkus integrierte Mobiltelefone zu Abhörzwecken. Dieser Sonderfall ist hierdurch nicht abgedeckt. Weitere Informationen hierzu siehe Kapitel 14.

M.5 Aufbewahrung

Die sichere Aufbewahrung des Endgeräts und insbesondere der SIM-Karte ist die wirksamste Maßnahme gegen Missbrauch der digitalen Identität eines Anwenders und gegen die Kompromittierung des Endgeräts.

M.6 Sperrung der SIM-Karten

Die SIM-Karte stellt die digitale Identität des Anwenders dar. Da das Kopieren von SIM-Karten denkbar ist (SIM-Cloning, definitiv nachgewiesen für SIM-Karten bis zum Jahr 1999), ist auch nach Wiederauffinden der zeitweise verlorenen SIM-Karte eine Kompromittierung denkbar. Eine sofortige Sperrung der SIM-Karte nach Bemerken des Verlusts ist grundsätzlich zu empfehlen, z. B. über die Hotline des Anbieters.

M.7 SIM-Lock

Viele Endgeräte können auf die Verwendung mit einer einzigen SIM-Karte beschränkt werden. Diese Maßnahme wird meist von Mobilfunk-Anbietern zur Sperrung vertragsgebundener Endgeräte eingesetzt. Hierdurch kann aber auch das Auslesen personenbezogener Daten unter Verwendung einer fremden SIM-Karte unterbunden werden. Dies ist allerdings nur in Verbindung mit der Verschlüsselung der auf dem Endgerät gespeicherten Daten wirksam (siehe M.77).

M.8 Mobiltelefonverbote

Ein Verbot der Mitnahme von Mobiltelefonen in Räumlichkeiten, in denen Gespräche mit vertraulichem Inhalt geführt werden, ist empfehlenswert. Eine entsprechende Kontrolle ist aufwendig und damit kostenintensiv, sollte aber zum Schutz vertraulicher Daten in Räumen mit erhöhtem Sicherheitsbedarf eingeführt werden.

M.9 Mobilfunkdetektoren

Einsatz passiver Warngeräte (GSM-Mobiltelefon-Detektoren) zur Aufspürung unerwünschter Mobiltelefone. Ein entsprechendes Gerät wird beispielsweise vom BSI vertrieben (siehe [BSIMDS]). Aktive Geräte und Störsender sind in Deutschland nicht zugelassen.

Sobald Daten gesendet werden, z. B. beim Anmelden, beim Abmelden, bei Gesprächen, beim Versenden von SMS, MMS oder beim Webbrowsing, ist das Handy aktiv und der gesendete Burst kann erkannt werden. Auf dieser Basis arbeiten Mobilfunkdetektoren, wie zum Beispiel der Mobilfunkdetektor MDS (siehe [BSIMDS]). Dieser Detektor erkennt nur Mobiltelefone im „sendenden“ Betriebszustand und kann so eine Mobilfunkkommunikation (GSM, UMTS und DECT (Digital Enhanced Cordless Telecommunication)) anzeigen.

Das Betreiben eines aktiven Mobilfunkdetektors, welcher selbst eine Funkzelle nachahmt und so das Telefon zum Senden auffordert, ist nach dem Telekommunikationsgesetz in Deutschland nicht zulässig. Das passive Detektieren hat jedoch den großen Nachteil, dass der Zeitpunkt nicht bestimmt werden kann, zu dem alle Telefone detektiert werden sollen. Ein möglicher Ansatz ist die Ausweitung der Mobilfunkdetektion auf die Location Updates. Damit werden auch Anmeldungen des Mobiltelefons in einer neuen Zelle registriert. Mithilfe eines Verstärkers, eines Transceivers und einer Richtfunkantenne, die das Signal einer weiter entfernten BTS auffängt, kann im lokalen Detektionsbereich das Signalverhältnis so beeinflusst werden, dass sich die Mobiltelefone an der nun stärker sendenden „gefälschten" Zelle anmelden. Der dabei notwendige Location Update „enttarnt" das Mobiltelefon und es wird detektiert. Bei diesem Vorgehen wird die Mobilfunkkommunikation nicht unterbunden, da der Aufbau alle vom Mobiltelefon gesendeten Daten an die entfernte BTS weiterleitet.

M.10 Verwendung von Prepaid-Karten zur Anonymisierung

Ein Kartentausch, der Erwerb von bereits registrierten SIM-Karten oder der Erwerb von Prepaid-SIM-Karten ohne Ausweisprüfung können zur Vermeidung der Identifikation beim Mobilfunkbetreiber genutzt werden. Diese Maßnahme verschleiert wirksam die Identität eines Mobilfunkteilnehmers. Im Geschäftsumfeld kann diese Maßnahme ergänzend für Mobilfunkteilnehmer mit erhöhtem Schutzbedarf durchgeführt werden.

M.11 Benachrichtigung der Überwachungsfunktion

Überwachungsdienstanbieter sind weder per Gesetz noch aus einer Selbstverpflichtung heraus an das Versenden einer Benachrichtigung gebunden. Diese Benachrichtigungs-SMS an das betroffene Endgerät setzt den Anwender über die Überwachung in Kenntnis. Darüber hinaus sollte die Überwachungsfunktion erst nach einer Freischaltung, z. B. durch eine Bestätigungs-SMS an den Diensterbringer, erfolgen.

M.12 Ortungsinformation

Ortungsdienstanbieter sind weder per Gesetz noch durch Selbstverpflichtung daran gebunden, über eine Ortung zu informieren. Systeme seriöser Dienstanbieter versenden bei einem Ortungsversuch eine Information über den Vorgang per SMS an die überwachten Endgeräte.

Abbildung 7: Ortungsdienste informieren überwachte Mobilfunkteilnehmer per SMS

2. GPRS, HSCSD und EDGE

Mit der Zunahme von mobilen Zugriffen auf Internet-basierte Dienste stießen die Mobilfunknetze an die Grenze ihrer Kapazitäten, da GSM ausschließlich für leitungsvermittelte Dienste wie Telefongespräche und Datenübertragung mit konstanter Datenrate (9.600 Bit/s) ausgelegt war. Daher wurden zusätzlich sowohl paketvermittelte Dienste im Hinblick auf die variablen Übertragungsraten als auch optimierte Modulationsverfahren zur Erhöhung des maximalen Durchsatzes geschaffen.

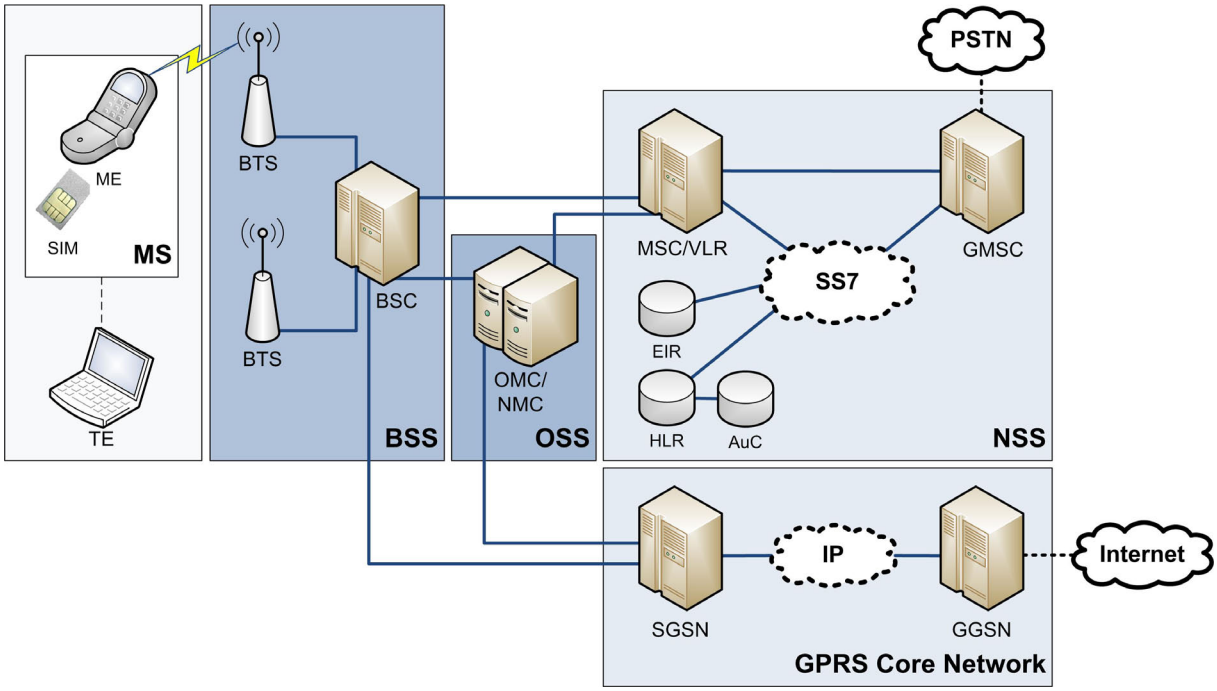
2.1 Technische Grundlagen

Im Folgenden werden die Übertragungsdienste GPRS und HSCSD sowie die EDGE-Technologie vorgestellt.

2.1.1 General Packet Radio Service

General Packet Radio Service (GPRS) ist ein paketvermittelter Dienst zur Datenübertragung über GSM-Verbindungen. GPRS wurde erstmalig durch das European Telecommunications Standards Institute (ETSI) standardisiert und in das GSM Release 97 integriert. Später übernahm das 3rd Generation Partnership Project (3GPP) die Weiterführung.

Abbildung 8: Einbettung des GPRS-Teilsystems in GSM-Netz (vereinfachte Darstellung)



Das GPRS-Netz ist als Parallelnetz zum leitungsvermittelten Teil des GSM-Netzes zu sehen. Als neue Elemente kommen der Serving GPRS Support Node (SGSN) sowie der Gateway GSN (GGSN) hinzu. Der SGSN hält eine logische Verbindung zum mobilen Endgerät aufrecht und ist unter anderem für das Routing sowie für das Handover des mobilen Endgeräts an

benachbarte SGSNs zuständig. Der GGSN ist unter anderem für die Zuweisung von IP-Adressen zuständig und stellt eine Schnittstelle zu Netzen außerhalb des GPRS-Netzes dar.

Die Funkverbindung selbst wird durch das GSM-Netz bereitgestellt. Die hierfür reservierten Frequenzbereiche sind mit denen von GSM identisch (siehe Tabelle 1). Das gesamte Multiplexing und Modulationsverfahren entspricht ebenfalls dem von GSM entsprechend Kapitel 1.1.1. Die effektive Bandbreite, die unter Nutzung eines der acht Zeitfenster des GSM-Rahmens zur Verfügung steht, ist für Datendienste sehr gering. Je nach Codierung beträgt die Bandbreite pro Zeitschlitz zwischen 8 und 20 kbit/s. Die unterschiedlichen Codierungsverfahren (Coding Schemes, CS) unterscheiden sich in ihrer Stabilität gegenüber Übertragungsfehlern. Je höher die zur Fehlerkorrektur benötigte Redundanzinformation ist, desto niedriger ist die effektive Datenrate. CS-1 verfügt über die beste, CS-4 über gar keine Fehlererkennung. Daher ist CS-4 selbst unter optimalen Bedingungen im Allgemeinen nicht einsetzbar. Die eingesetzte Codierung wird dem übertragungstechnischen Bedürfnis nach Fehlerkorrektur dynamisch angepasst.

Tabelle 2: Für GPRS gebräuchliche Codierungen

Codierung (Coding Scheme, CS)	Redundanzinformationen (prozentual)	Datenübertragungsrate (pro genutztem Zeitschlitz)
CS-1	60 %	8,0 kbit/s
CS-2	40 %	12,0 kbit/s
CS-3	28 %	14,4 kbit/s
CS-4	0%	20,0 kbit/s

Damit trotz niedriger Nettodatenrate eines Zeitschlitzes brauchbare Durchsätze erreicht werden, ermöglicht GPRS die dynamische Nutzung von bis zu vier der acht Timeslots für den Downlink (BTS => Endgerät) und zwei für den Uplink (Endgerät => BTS). Maximal lassen sich hiermit bei Codierung entsprechend CS-3 56,6 kbit/s auf dem Downlink erreichen. Die Fähigkeit zur Nutzung mehrerer Zeitslots hängt vom verwendeten Endgerät ab (englisch multislot capability). Die Zahl der genutzten Zeitscheiben wird durch einen Klassenbezeichner zusammengefasst. Multislot Class 1 steht dabei für einen Slot Uplink und einen Slot Downlink. Bekannte Implementierungen bieten maximal Multislot Class 10, was dem oben beschriebenen Verfahren mit vier Slots Downlink und zwei Slots Uplink entspricht.

Tabelle 3: Multislot-Klassen für Mobile Endgeräte

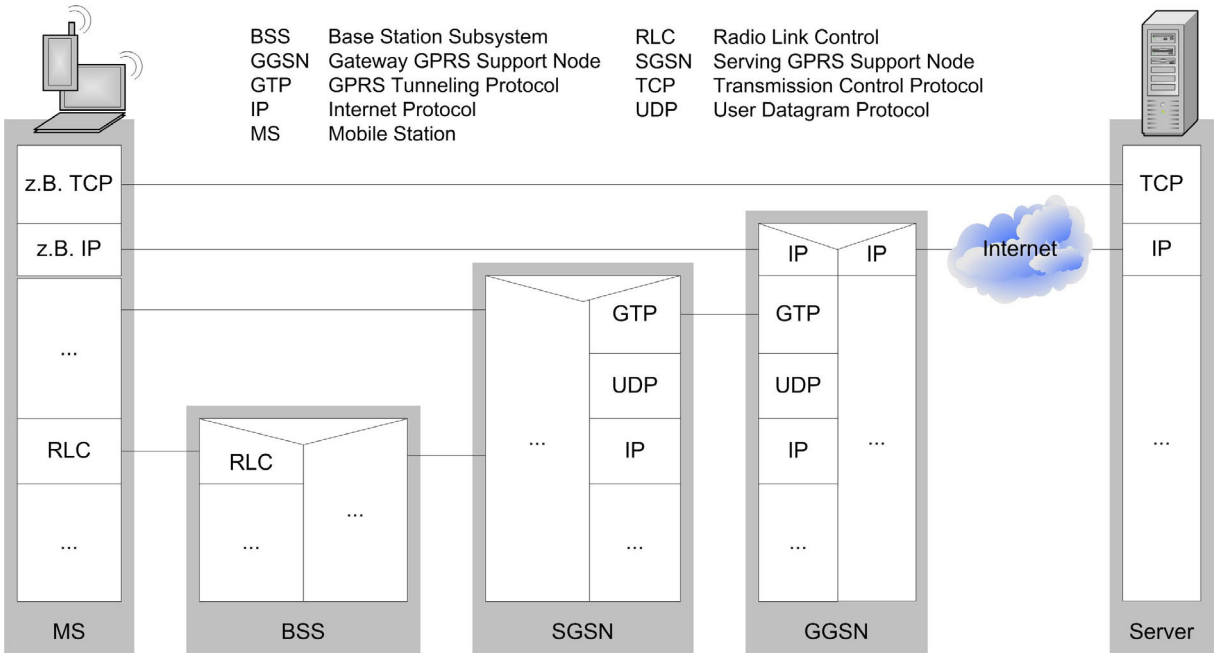
Multislot Class	Max. Slots (Downlink)	Max. Slots (Uplink)	Max. aktive Slots
1	1	1	2
2	2	1	3
3	2	2	3
4	3	1	4
…			
10	4	2	5

Multislot Class	Max. Slots (Downlink)	Max. Slots (Uplink)	Max. aktive Slots
…			
45	6	6	7

Im Gegensatz zu leitungsvermittelten Diensten (Circuit Switched Services), welche in der Regel nach Zeiteinheiten abgerechnet werden, erfolgt die Abrechnung des GPRS-Datenverkehrs nach Übertragungsvolumen. Auf diese Weise kann kostengünstig eine (virtuelle) dauerhafte Verbindung bereit gestellt werden, da der Funkraum nur dann durch GPRS in Anspruch genommen wird, wenn Daten übertragen werden. Dieses paketorientierte Verfahren (englisch packet switched) bietet Vorteile in Bezug auf die Ausnutzung der Übertragungskapazitäten des Funkraums. Somit eignet sich GPRS besonders gut für Dienste wie beispielsweise Push Mail, Internet Browsing, Instant Messaging usw.

Die Kompatibilität zu IP-basierten Netzen (Internet Protocol) wird bei GPRS erst in höheren Schichten des Protokollstapels realisiert. Darunterliegend kommt eine Reihe von (teilweise) auf den Einsatz in Mobilfunknetzen spezialisierten Protokollen zum Einsatz, wie in Abbildung 9 veranschaulicht ist. Zwischen Endgerät und BSS existiert eine Layer-2-Verbindung basierend auf dem Protokoll Radio Link Control (RLC). Auch zwischen BSS, SGSN und GGSN kommen unterschiedliche Schichtungen aus verschiedenen Medien und Protokollen zum Einsatz. Auf diesen insgesamt fünf Protokollschichten wird nun zwischen GGSN und Endgerät als sechste Schicht IP realisiert. Interessant ist hierbei, dass in den tieferen Schichten zwischen SGSN und GGSN bereits IP zum Einsatz kommt. Hierauf setzt das UDP-basierte (User Datagram Protocol) GPRS Tunnelling Protocol (GTP) auf, in welchem die IP-Pakete zum GGSN getunnelt werden. Erst in der siebten Schicht existiert eine Layer-4 Verbindung (z. B. Transport Control Protocol, TCP) zwischen Endgerät und Endpunkt im Internet, gemäß ISO-OSI-Referenzmodell.

Abbildung 9: GPRS-Datenübertragung



Da die tatsächlich verfügbare Bandbreite in Abhängigkeit von der gleichzeitigen Nutzung durch andere Mobilfunkteilnehmer ständig schwanken kann, ist GPRS weniger geeignet für Streaming-Dienste als ein leitungsvermittelter Übertragungsdienst (siehe Kapitel 2.1.2). Ein Vorteil dieser virtuellen Verbindung ist die Möglichkeit, während eines Gesprächs per GSM die Datenverbindung zu halten und nach dessen Ende die Sitzung ohne erneuten Verbindungsaufbau fortzusetzen. Für die Datenübertragung per GPRS werden dabei dieselben Zeitslots (siehe Kapitel 1.1.2) genutzt wie für das Telefongespräch.

2.1.2 Circuit Switched Data und HSCSD

Circuit Switched Data (CSD) und High Speed CSD (HSCSD) basieren wie GPRS auf dem GSM-Netz, d. h. Multiplexing und Modulation sind identisch. Im Gegensatz zu GPRS sind CSD und HSCSD allerdings leitungsvermittelte Dienste. Das heißt, die entsprechenden TDMA-Zeitschlitze werden nicht dynamisch belegt, sondern statisch für die Verbindung reserviert. Während das kaum mehr relevante CSD lediglich jeden achten Slot nutzen kann (1:1, Multislot Class 1), ist HSCSD in der Lage mehrere Zeitschlitze zu nutzen. Hierfür stehen die Slotbelegungen nach Klasse 2 und 4 (2:1 und 3:1), entsprechend Tabelle 3 zur Verfügung. Damit werden Datenraten von 28,8 bzw. 43,2 kbit/s Downlink und 14,4 kbit/s Uplink erreicht.

Diese asymmetrische, aber statische Kanalbündelung von HSCSD eignet sich besonders für Streaming Dienste, die in der Regel eine dauerhafte Verbindung mit konstanter Bandbreite erfordern. Da HSCSD leitungsvermittelt ist und dauerhaft Bandbreite belegt, wird es in den meisten Fällen nach Verbindungsdauer und nicht nach transferiertem Datenvolumen abgerechnet. Für Dienste, in denen nur punktuell Daten übertragen werden (z. B. Push Mail) empfiehlt sich daher eher der Einsatz von GPRS.

2.1.3 Enhanced Data Rates for GSM Evolution

Enhanced Data Rates for GSM Evolution (EDGE) dient der Erhöhung der Datentransferrate in GSM-Mobilfunknetzen. Hierbei sind zwei Kombinationsmöglichkeiten in Betracht zu ziehen. Einmal eine Kombination aus GPRS und EDGE, das sogenannte EGPRS (Enhanced GPRS), oder eine Kombination aus HSCSD und EDGE (ECSD). EDGE basiert vollständig auf GSM, mit identischem Multiplexverfahren. Um nun höhere Datenraten zu ermöglichen, wird bei EDGE ein alternatives Modulationsverfahren eingesetzt. EDGE ist also in seiner Funktionsweise zwischen GSM und GPRS bzw. HSCSD angesiedelt. Das Sendesystem ist komplett mit dem GSM-Netz identisch und besteht ebenfalls aus mehreren Sende- und Empfangsstationen (Base Transceiver Station, BTS) sowie einem Base Station Controller (BSC). Die Summe aller BSS bildet das GSM-Funknetz GSM EDGE Radio Access Network (GERAN). Jedes dieser Systeme ist mit dem Vermittlungssystem des jeweiligen Netzbetreibers verbunden. Sämtliche Kommunikation des mobilen Endgerätes hinsichtlich Authentisierung, Verbindungsaufbau, Datenübermittlung usw. läuft über das Network Subsystem (NSS). Eine detaillierte Beschreibung der Struktur des GERAN findet sich unter Kapitel 1.1.1.

Während bei GSM standardmäßig die Gaußsche Minimalphasenmodulation (GMSK) verwendet wird, basiert EDGE auf achtfachem Phase Key Shifting (8-PSK). Wo bei GMSK pro Symbol nur 1 Bit übertragen werden kann, sind dies bei 8-PSK 3 Bit, was $2^3 = 8$ Zuständen je Symbol entspricht. Damit ließen sich prinzipiell Datenraten bis zur dreifachen GSM-Geschwindigkeit erreichen. Jedoch wird für das differenziertere Modulationsverfahren ein

höheres Signal-Rauschleistungsverhältnis (Signal Noise Ratio, SNR) bei der Funkübertragung benötigt. Dies betrifft sowohl die sender- als empfängerseitige Signalverarbeitung. Ein höheres SNR wird durch eine bessere Rauschleistungsanpassung der zur Übertragung eingesetzten Schaltungen, also der Optimierung der Signalübertragung für minimales Rauschen, erreicht. Damit dies nicht zu Lasten der Leistung des Signals – und somit zu Lasten der Reichweite der Funkverbindung – geht, ist eine höhere Güte der eingesetzten Technologie notwendig. Doch auch dies ist keine Garantie für die korrekte Übertragung aller Symbole, was den Einsatz von Codierungsverfahren mit höherer Redundanz erfordert. So wird pro Kanal eine Datenrate zwischen 22,4 kbit/s (CS-5) und 59,2 kbit/s (CS-9) erreicht, wobei CS-9 der Codierung mit der schwächsten Fehlerkorrektur entspricht (siehe Tabelle 4).

Tabelle 4: Für EDGE gebräuchliche Codierungen

Codierung (Coding Scheme, CS)	Redundanzinformationen (prozentual)	Datenübertragungsrate (pro genutztem Zeitschlitz)
CS-5	63 %	22,4 kbit/s
CS-6	51 %	29,6 kbit/s
CS-7	24%	44,8 kbit/s
CS-8	8 %	54,4 kbit/s
CS-9	0 %	59,2 kbit/s

Für den Einsatz des verbesserten Modulationsverfahrens ist ein Austausch älterer BTS durch den Provider notwendig. EDGE wird daher bislang nur durch wenige Provider flächendeckend eingesetzt. Die Einführung von EDGE geschieht oft bei der Neuerschließung von Gebieten oder beim Austausch veralteter BTS. Die Technologie bietet aber gerade im Bereich der Kosten einige Vorteile für Provider. Da sogar innerhalb des TDMA-Verfahrens für jeden Zeitslot zwischen GMSK und 8-PSK gewechselt werden kann, ist kein Einsatz zweier verschiedener BTS notwendig. Auch Investitionen in die restliche Infrastruktur entfallen, da abgesehen von den BTS die Technologie identisch ist. EDGE wird daher gern als kostengünstigere Alternative zu UMTS oder als Fallback-Technologie in schwach ausgebauten Gebieten eingesetzt.

2.2 Sicherheitsgefährdungen

Zusätzlich zu den GSM-spezifischen Sicherheitsgefährdungen kommen bei der Nutzung von Datenverbindungen neue Gefährdungen hinzu, welche im Folgenden angesprochen werden.

2.2.1 General Packet Radio Service

Die GPRS-Datenübertragung erfolgt beispielsweise beim Zugriff auf einen Server über das Internet mittels TCP/IP (siehe Abbildung 9). Somit kommen hier sämtliche Gefährdungen innerhalb IP-basierter Netze hinzu (siehe [GSKBSI]).

Es erfolgt analog zur Vorgehensweise innerhalb GSM-Netzen eine Authentisierung gegenüber dem Dienstanbieter sowie eine Verschlüsselung der Kommunikation unter Verwendung des GEA (GPRS Encryption Algorithm). Hierbei übernimmt das SGSN die Rolle des MSC.

Die Verschlüsselung geschieht auf dem LLC Layer (Logical Link Control Layer) zwischen MS und SGSN. Die Sicherheit der Übertragung zwischen SGSN und GGSN liegt im Verantwortungsbereich des Netzbetreibers. Der unsichere Bereich (Internet) beginnt am GGSN.

Somit ist auch bei der Nutzung von GPRS analog zu GSM eine Ende-zu-Ende-Verschlüsselung zur Sicherung vertraulicher Daten zwingend notwendig.

2.2.2 HSCSD und EDGE

HSCSD und EDGE sind Übertragungsdienste ohne eigene Methoden zur Authentisierung, Verschlüsselung usw., welche bereits beim Aufbau der GSM-Verbindung durchgeführt werden. Somit kommen aus dieser Hinsicht keine zusätzlichen Gefährdungen hinzu.

Zusätzliche Gefährdungen entstehen allerdings durch die Tatsache, dass hier Datenverbindungen aufgebaut und weitere Protokolle und Dienste genutzt werden (z. B. WAP, MMS usw.). Die durch solche zusätzliche Dienste bedingten Gefährdungen werden im Kapitel 8 beschrieben.

Weiterhin bieten die mithilfe von HSCSD und EDGE möglichen höheren Datenübertragungsraten auch neue Möglichkeiten des Missbrauchs und der Überwachung, wie beispielsweise die Übertragung von Bildmaterial. Ein mit einer (unauffälligen) Kamera ausgestattetes Mobiltelefon kann als Spionage-Instrument benutzt werden. Die garantierte Bandbreite von HSCSD eignet sich beispielsweise für das Streaming von Sprachdaten, während EDGE mit seiner höheren Datenrate in Form von ECSD bedingt sogar für Videostreaming geeignet ist. Die höhere Bandbreite erlaubt es auch, hochauflösende Bildaufnahmen zeitnah zu versenden. Darüber hinaus ist die Anwendung der Steganographie denkbar, die Informationen verborgen in unverdächtigen Bildern oder Texten speichert, um Daten unbemerkt zu übermitteln.

2.3 Mögliche Schutzmaßnahmen

Generell sollten bei Verwendung von GPRS, HSCSD und EDGE dieselben Schutzmaßnahmen ergriffen werden, die auch bei Nutzung von IP-basierten Diensten empfohlen werden. Darüber hinaus kann der Nutzer unerwünschte und eventuell kostenintensive oder gefährdete Dienste für seinen Anschluss vom Netz-/Dienstbetreiber deaktivieren lassen. Ein Beispiel für einen deaktivierbaren, kostenintensiven Dienst ist HSCSD in Roaming-Netzen.

Im Vergleich zu GPRS sind für EDGE keine weiteren Schutzmaßnahmen erforderlich. Jedoch führt eine höhere Datenrate potenziell zu einer intensiveren Nutzung von Online-Diensten, was das Schutzbedürfnis tendenziell erhöht. Eine erhöhte Datenübertragungsrate könnte allerdings im Gegenzug für stärkere Verschlüsselungsverfahren genutzt werden.

Die Maßnahmen, die zum Schutz bei der Nutzung von mobilen Online-Diensten ergriffen werden können, werden in den Kapiteln 8, 10 und 12 näher erläutert. Mögliche Schutzmaßnahmen werden direkt unter den jeweiligen Diensten genannt.

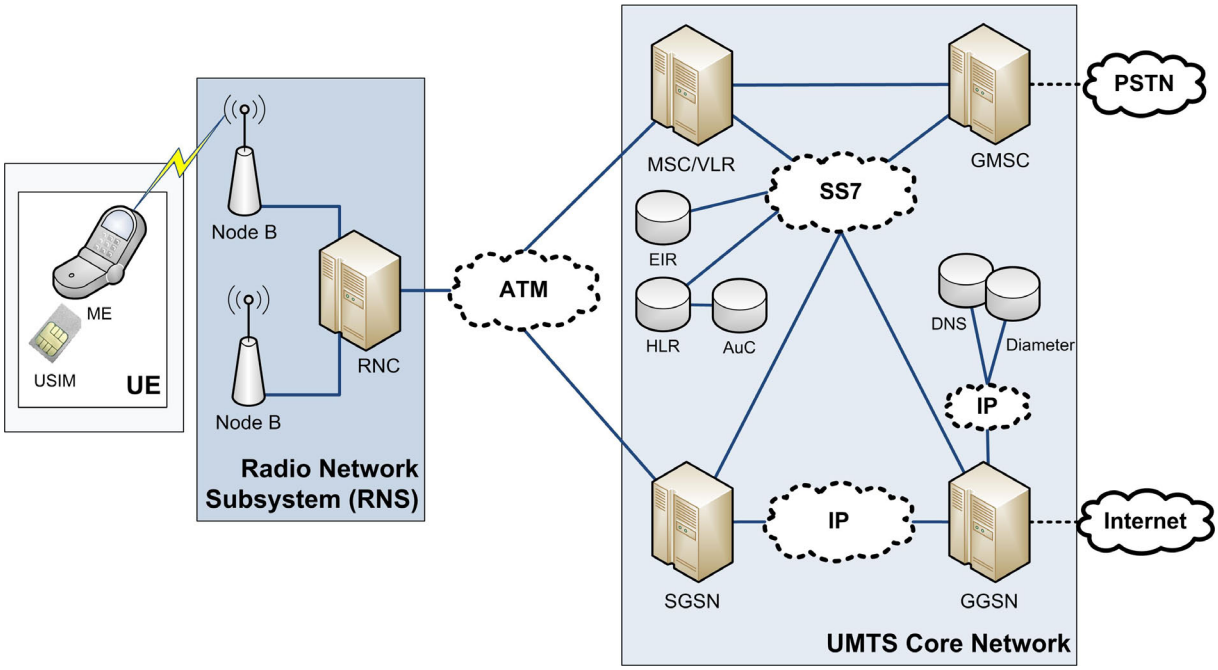
3. Universal Mobile Telecommunication System

Das Universal Mobile Telecommunication System (UMTS) stellt den Schritt in die dritte Generation mobiler Kommunikationssysteme (3G) dar. Die erreichbaren Übertragungsgeschwindigkeiten für Daten liegen im Bereich von 144 kbit/s bis zu 384 kbit/s und bieten somit eine Basis für breitbandige multimediale Kommunikations- und Informationsdienste.

3.1 Technische Grundlagen

UMTS wurde erstmals innerhalb der GSM-Phase 2+ / UMTS Release 99 standardisiert. Anschließend wurden die Releases 4, 5 und 6 veröffentlicht. Seit der Veröffentlichung von Release 6 im Jahr 2006 wird an Release 7 gearbeitet. Die Implementierung neuer Releases wird in den Mobilfunknetzen der unterschiedlichen Betreiber unterschiedlich schnell durchgeführt. In der Regel beträgt die Verzögerung mehrere Jahre. Daher bezieht sich die folgende Beschreibung zunächst auf den ursprünglichen Release 99.

Abbildung 10: Vereinfachte Darstellung der UMTS-Netzarchitektur nach Release 99



Der Aufbau der UMTS-Netzarchitektur ist dem Aufbau von GSM/GPRS Netzen zunächst sehr ähnlich (siehe Kapitel 1.1.1). Dies wird insbesondere bei der vereinfachten Darstellung in Abbildung 10 deutlich. Dennoch bestehen technische Unterschiede in diversen Teilbereichen sowie in der Nomenklatur.

3.1.1 UMTS Core Network

Wie Abbildung 10 zu entnehmen ist, vereint das UMTS Core Network sowohl Komponenten analog zu GSM in einem leitungsvermittelten SS7-Netz als auch Komponenten analog zu GPRS in einem paketvermittelten IP-Netz. Die einzelnen Komponenten sowie die Schnittstellen zu externen Netzen entsprechen weitestgehend den Beschreibungen in Kapitel 1 und 2.

Zum Beispiel ist das GGSN – wie auch in der GPRS-Architektur – für die Anbindung an externe paketbasierte Netze und für die Nutzungsabrechnung zuständig. Dafür ist das GGSN mittels Gateway an das sogenannte Billing Center angebunden, in dem alle abrechnungsrelevanten Daten zusammenlaufen. Auch die Anbindung an andere Providernetze wird über das GGSN realisiert. Die Vorgaben des UMTS Release 99 werden auch in ausländischen Providernetzen auf dieselbe Weise realisiert; Gefährdungen und Sicherheitsmaßnahmen entsprechend also auch den hier angegebenen.

Allerdings finden sich auch einige Unterschiede zur GSM/GPRS-Architektur, insbesondere in den Protokollschichten finden sich einige Abweichungen. Das GTP-Protokoll wird nicht nur zum Transport zwischen GGSN und SGSN verwendet, sondern auch in der Kommunikation zwischen SGSN und RNC (Radio Network Controller). Dies resultiert aus der Auslagerung der Medienzugriffskontrolle (Media Access Control, MAC) in die RNCs.

3.1.2 Modulation und Codierung

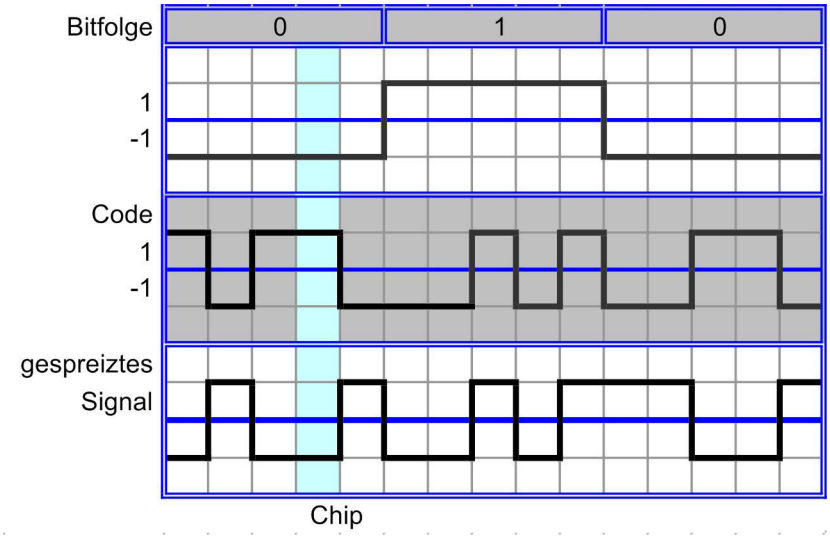
Die Unterschiede zu GSM beginnen bereits auf der Luftschnittstelle. Die für die Nutzung durch UMTS in Deutschland lizenzierten Frequenzen liegen zwischen 1920,3 und 1979,7 MHz für den Uplink und zwischen 2110,3 und 2169,7 MHz für den Downlink. Hier wurden sechs je 10 MHz breite Frequenzbänder definiert, von denen vier bereits an verschiedene Netzbetreiber lizenziert wurden. Hierdurch ergeben sich pro Betreiber je zwei Frequenzbereiche à 5 MHz für Up- und Downlink. Zugrunde liegt das sogenannte Frequency Division Duplex (FDD), bei dem Up- und Downlink in verschiedenen Frequenzbereichen stattfinden. Im Gegensatz hierzu ermöglicht Time Division Duplex (TDD) die Unterteilung eines Zeitrahmens von 10 ms in 15 Zeitscheiben (ähnlich TDMA bei den Multiplexverfahren), die dann abwechselnd für Uplink und Downlink verwendet werden. TDD ist ebenfalls für UMTS standardisiert, die deutschen Netzbetreiber setzen beim Netzaufbau aber auf FDD.

Die Kanäle werden auf diese Frequenzen per Wideband Code Division Multiple Access (W-CDMA) aufmoduliert. W-CDMA ist ein sogenanntes Code-Multiplexverfahren. Das „Wideband“ steht für eine Verteilung des übertragenen Signals auf ein breites Frequenzspektrum. Code-Multiplexverfahren unterteilen nun diesen breiten Frequenzraum nicht in feste Frequenzkanäle oder in Zeitscheiben wie FDMA oder TDMA. Stattdessen senden alle Sender im selben Frequenzbereich. Um die einzelnen Datenströme zu extrapolieren, bedient man sich eines mathematischen Verfahrens, dem Code-Multiplexing.

Jedem Empfänger wird eine sogenannte Spreizsequenz zugewiesen. Diese ist eindeutig und besteht aus einer binären Folge im NRZ-Format (Non Return Zero, also „-1“ und „+1“ als Wertebereich). Die zu codierende Bitfolge wird für die Codierung ebenfalls im NRZ-Format dargestellt. Nun werden Bitfolge und Spreizcode miteinander multipliziert (Vektoroperation) und man erhält als Ergebnis das codierte (gespreizte) Signal (siehe Abbildung 11). Der Empfänger verfügt ebenfalls über Kenntnis der Spreizsequenz und kann die ursprüngliche Bitfolge somit leicht rekonstruieren. Die Intelligenz in diesem Verfahren liegt in der Auswahl der Spreizsequenz. Jede verfügbare Spreizsequenz ist zu jeder anderen im mathematischen Sinne orthogonal. Eine Eigenschaft von zueinander orthogonalen Vektoren ist, dass ihr Produkt immer null wird. So wird jede Codesequenz, die mit einem anderen als dem eigenen Spreizcode codiert wurde, bei der Decodierung ebenfalls zu null. Die von anderen Teilnehmern gesendeten Daten sind also für das Endgerät „unsichtbar“. So ist auch bei Überlagerung vieler

codierter Signale eine eindeutige Unterscheidung der Datenströme möglich. Dieses Verfahren garantiert eine sehr gute Ausnutzung der verfügbaren Frequenzbereiche.

Abbildung 11: CDMA - Bitfolge, Spreizcode und codiertes („gespreiztes“) Signal



Als Modulationsverfahren kommt momentan QPSK (Quadrature Phase Key Shifting), ein auch als 4-PSK bezeichnetes Phasenmodulationsverfahren, zum Einsatz. Im Gegensatz zu GMSK (GSM, 1 Bit pro Symbol) und 8-PSK (EDGE, 3 Bit pro Symbol) werden hierbei 2 Bit pro Symbol aufmoduliert. Ein zukünftiger Einsatz von 8-PSK zur Erhöhung der Datenrate wäre ebenfalls denkbar.

Zur Codierung von Sprachdaten unter UMTS wurde vom 3GPP-Forum der Adaptive Multirate Wideband Codec (AMR-W) vorgeschlagen. Diese Erweiterung des auch schon unter GSM einsetzbaren AMR ermöglicht eine höhere Bandbreite des codierten Sprachsignals (50 Hz bis 7 kHz, statt bislang 300 Hz bis 3,4 kHz). Der Codec ist adaptiv, d. h. er passt sich innerhalb gewisser Grenzen der verfügbaren Datenrate an und fügt bei höherer Fehlerrate Redundanzinformationen hinzu, um die Sprachqualität zu stabilisieren. Bislang wird in der Regel auf AMR zurückgegriffen, AMR-W ist jedoch bereits bei einigen Anbietern in der Erprobungsphase und wird voraussichtlich noch 2008 eingeführt.

3.1.3 User Equipment

User Equipment (UE) bezeichnet das mobile Endgerät, das in der Regel aus einem Mobiltelefon (Mobile Equipment, ME) und einer Universal Integrated Circuit Card (UICC) oder einer herkömmlichen SIM-Karte besteht. Die UICC ist eine Smartcard, die in Mobilfunknetzen der dritten Generation die bei GSM genutzte SIM-Karte ersetzt. Sie hat die Aufgabe, nutzerspezifische Daten zu speichern und Routinen zur Authentifizierung bereit zu stellen. Der wesentliche Unterschied zur SIM-Karte besteht in der Möglichkeit, mehrere Anwendungen gleichzeitig ausführen zu können, was z. B. Funktionalitäten wie Signierung oder bargeldloses Bezahlen ermöglicht. Die bei GSM bisher von der SIM-Karte erbrachten Funktionen, wie Authentifizierung gegenüber dem GSM-Netz, werden auf der UICC vom Universal Subscriber Identity Module (USIM) übernommen.

Das USIM ist der Nachfolger der im GSM-Umfeld genutzten SIM-Karte. Wann welcher Netzbetreiber auf das USIM umstellen wird, steht zum jetzigen Zeitpunkt noch nicht fest. Es

werden in Zukunft durchaus noch herkömmliche SIM-Karten von Seiten der Betreiber ausgegeben. Ebenso wie auf dem SIM werden im USIM benutzerspezifische Informationen und Daten gespeichert, allerdings verfügt das USIM insbesondere über erweiterte Sicherheitsfunktionen. So wird bei der Personalisierung im USIM zur Authentisierung ein 128 Bit langer Schlüssel K gespeichert. Dieser ist ebenfalls beim Home Location Register (HLR) des Netzes hinterlegt. Weiterhin beinhaltet USIM verschiedene Algorithmen, die zur Authentisierung und zur Verschlüsselung der Daten und Signalisierungsinformationen dienen. Aus Sicherheitsgründen wird zusätzlich eine Sequenznummer (SQN) im USIM gespeichert, die Rückschlüsse auf die mehrmalige Verwendung der Sitzungsschlüssel liefert. Der verwendete Verschlüsselungsalgorithmus ist der KASUMI block cipher aus A5/3. Unter Verwendung von ebenfalls vom USIM dynamisch generierten Sitzungsschlüsseln CK und IK werden die über die Luftschnittstelle gesendeten Informationen zwischen dem ME und dem Radio Network Controller (RNC) verschlüsselt. Somit bietet USIM eine höhere Sicherheit als SIM.

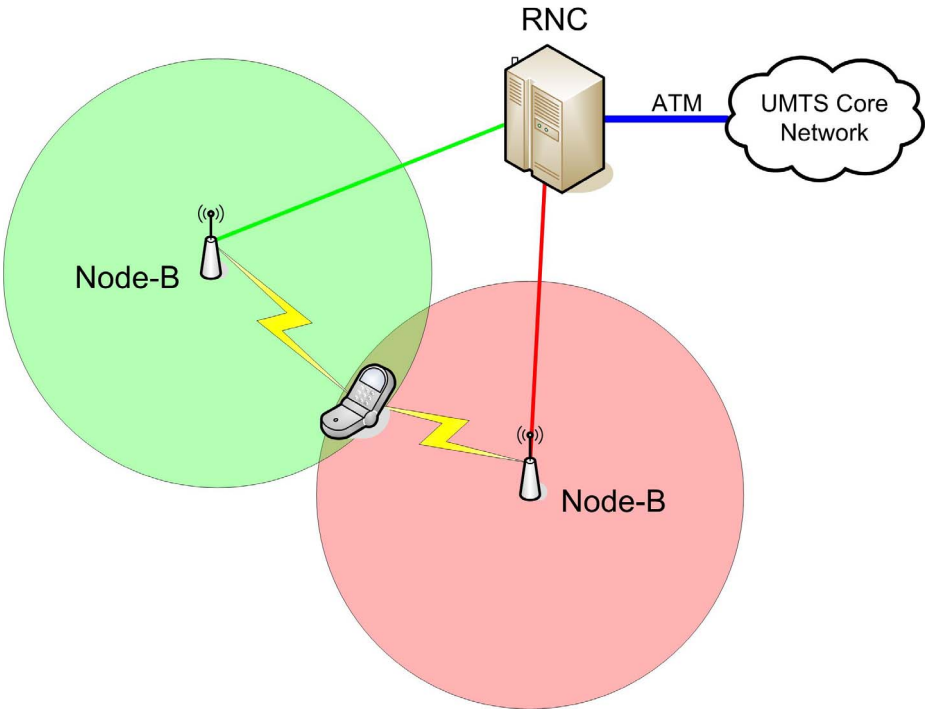
Wie auch bei GSM-Netzen erfolgt die Authentisierung des Nutzers gegenüber der USIM durch Eingabe einer PIN nach Start des Endgerätes, der erfolgreichen Wahl eines Netzes und dem Wechsel in den Zustand „Idle“. Die USIM authentifiziert sich dann gegenüber dem Betreibernetz, woraufhin bei Erfolg der Zustand „Connected“ erreicht wird. Ab diesem Zeitpunkt stellt die USIM die digitale Identität des Anwenders gegenüber dem Providernetz dar.

3.1.4 Radio Network Subsystem

Das mobile Endgerät baut über die Luftschnittstelle eine Verbindung mit einer Basisstation auf, um sich in das Betreibernetz zu integrieren. Jede Basisstation gehört zu einem Subnetz des Funknetzes UMTS Terrestrial Radio Access Network (UTRAN). Diese Subnetze werden Radio Network Subsystem (RNS) genannt und bestehen in der Regel aus mehreren Location Areas (LA). Diese wiederum enthalten mehrere Sende- und Empfangsstationen (Node-B, entspricht BTS in der GSM-Nomenklatur) sowie einen Radio Network Controller (RNC). Jeder RNC ist an das UMTS Core Network (CN) angebunden und stellt den Zugriff auf darin gebotene Dienste sicher. Außerdem realisiert der RNC die von UMTS geforderte sogenannte Makro-Diversität.

Makro-Diversität ist ein Verfahren, das Schwächen des oben beschriebenen W-CDMA bei überlappenden Funkzellen ausgleicht. Befindet sich ein Sender im Überlappungsbereich, so stellt seine erhöhte Sendeleistung eine deutliche Störung der benachbarten Funkzelle dar. Statt nun die Sendeleistung der in der benachbarten Zelle befindlichen Teilnehmer zu erhöhen, was bei W-CDMA die verfügbare Kapazität der Funkzelle erheblich schmälert, baut das Endgerät einen zweiten Kanal über die benachbarte Funkzelle auf. Darüber werden exakt dieselben Daten gesendet wie über die bestehende Verbindung. Die Daten werden als Redundanzinformationen genutzt und im RNC zusammengeführt. So ist es nicht notwendig, die Sendeleistung des Endgeräts anzuheben, wodurch die Störung der benachbarten Zelle minimiert wird.

Abbildung 12: Makro-Diversität im Überlappungsbereich zweier Basisstationen



Im Gegensatz zu GSM können in der UMTS-Architektur mehrere RNC in einem logischen RNS enthalten sein. Die RNC und damit auch die LA sind direkt untereinander vernetzt. Dem Teilnehmer wird im Visitor Location Register keine Node-B zugeordnet, sondern eine LA. Das ermöglicht zum einen die sanfte Übergabe (Soft Handover) nicht nur zwischen Funkmasten einer Node-B, sondern auch zwischen einzelnen Node-B innerhalb derselben LA. Aber auch die Übergabe von mobilen Teilnehmern zwischen den LA kann durch die Vernetzung der RNC ohne erneute Anmeldung erfolgen.

3.1.5 Roaming

Das Roaming in UMTS-Netze anderer Anbieter ist technisch problemlos. Über paketbasierte Datenverbindungen können Daten aus den Zugriffsnetzen von Drittanbieter weltweit in das Heimatnetz weitervermittelt werden. Die technische Umsetzung der Sicherheitsfunktionen unterscheidet sich international nicht, da als Basis gleichermaßen der UMTS-Standard dient. Allerdings ist die Rechtslage zum Datenschutz bei Weitem nicht in allen Ländern identisch. Hier ist es ratsam, sich vor der Nutzung über die geltenden Datenschutzbestimmungen zu informieren. Die Mechanismen im UMTS-Netz für die sogenannte Lawful Interception könnten einem möglicherweise nicht vertrauenswürdigen Personenkreis zur Verfügung stehen.

Hinzu kommen die hohen Roaming-Gebühren, die bei der Nutzung von UMTS im Ausland anfallen. Obwohl auf technischer Seite geringer Aufwand für die Durchleitung der Daten durch fremde Netze entsteht, werden hier oftmals hohe Tarife abgerechnet. Dies muss bei einer Nutzung von UMTS im Ausland berücksichtigt werden.

3.2 Sicherheitsfunktionen

Mit der Standardisierung von UMTS wurden wesentliche Verbesserungen im Bereich der Sicherheitsfunktionen im Vergleich zu GSM vorgenommen. Im Folgenden werden die wichtigsten Neuerungen vorgestellt.

3.2.1 Authentisierung und Verschlüsselung

UMTS verfügt über einen verbesserten Authentication and Key Agreement (AKA) Mechanismus. Bei der Implementierung wurde darauf geachtet, dass die Kompatibilität zu GSM gewahrt und die Migration von GSM zu UMTS so einfach wie möglich gehalten ist.

Eine erweiterte Sicherheitsfunktion ist die Authentisierung des Mobilfunknetzes gegenüber dem Mobilfunkteilnehmer durch ein gegenseitiges Challenge-Response-Verfahren. Damit wird die Sicherheitsgefährdung, die von einem „IMSI-Catcher“ ausgeht, behoben (siehe G.12). Dazu wurde das AKA um ein sogenanntes Authentication Token (AUTN) erweitert, welches im ersten Schritt der Anmeldung verifiziert wird. Nur wenn das AUTN gültig ist, d. h. die Identität des Mobilfunkbetreibers sichergestellt ist, wird die Teilnehmer-Authentifizierung durchgeführt. Dies hat zur Folge, dass ein möglicher Angreifer mit einem ungültigen AUTN keine Daten zur Teilnehmer-Authentifizierung abfangen kann und demnach auch keine Möglichkeit besitzt, den geheimen Identitätsschlüssel K des Mobilfunkteilnehmers zu rekonstruieren, wie es bei GSM möglich war. Es wird lediglich eine „user authentication reject“-Nachricht an das VLR gesendet.

Die verbesserte Sicherheit benötigt, wie schon im vorhergehenden Kapitel angedeutet, mehr Daten als bei GSM. Wo bei GSM nur drei Werte benötigt wurden, sind es bei UMTS schon fünf. Diese Datensätze werden in einem sogenannten authentication vector (AV) gespeichert, der jeweils nur mit einer USIM, genauer mit dem einmaligen Identitätsschlüssel K, verwendet werden kann. Für jeden Teilnehmer werden bei einer Authentisierungs-Anfrage (authentication data request) vom VLR oder SGSN ans HLR mehrere AVs vom AuC generiert und im authentication data response (AV_1, AV_2, …, AV_n) zurückgesendet.

In einem AV sind folgende Daten enthalten:

- RAND – eine nicht vorhersagbare 128 Bit lange Zufallszahl (auch bei GSM)
- XRES – Expected Response zur Teilnehmer-Authentifizierung (bei GSM SRES 32 Bit)
- CK – Ciphering Key 128 Bit für die Verschlüsselung (bei GSM Kc 64 Bit)
- IK – Integrity Key 128 Bit für die Datenintegrität
- AUTN – Authentication Token 128 Bit zur Netz-Authentifizierung

Es werden mehrere AVs zurückgesendet, die im VLR/SGSN gespeichert werden, um bei erneuten Authentisierungs-Anfragen bzw. Änderungen der verwendeten Verschlüsselung zeitnah zu handeln. Das 128 Bit lange Authentication Token selbst besteht nochmals aus drei Werten:

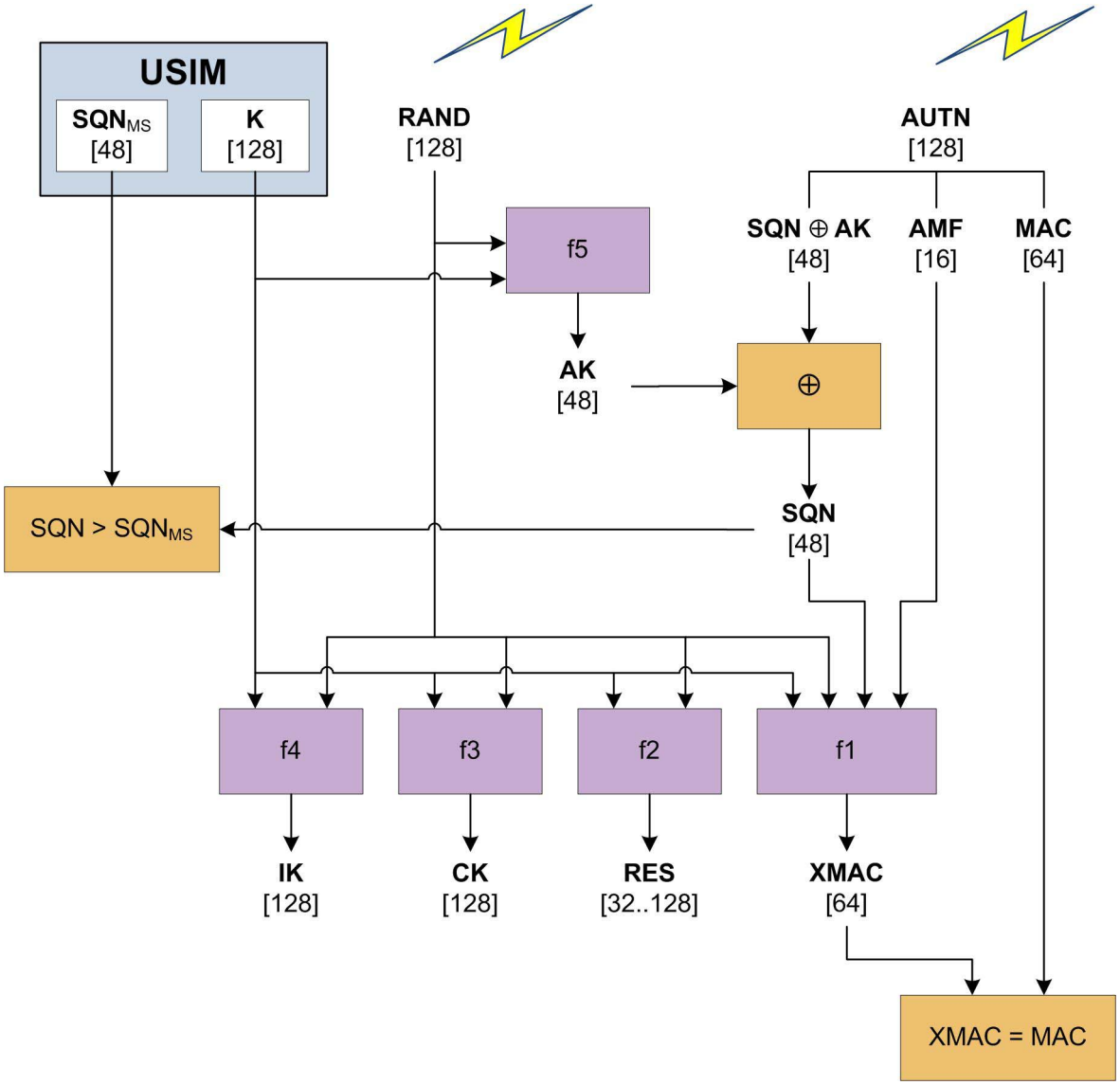
- SQN ⊕ AK – die verschleierte 48 Bit lange Sequenznummer (SQN) mittels XOR Verknüpfung mit dem 48 Bit langen Anonymity Key (AK)
- AMF – Authenticated Management Field 16 Bit
- MAC – Message Authentication Code 64 Bit zur Authentifizierung des Netzs

Im AUTN ist die SQN verschleiert, da sie Rückschlüsse über den Mobilfunkteilnehmer und dessen Aufenthaltsort liefern kann.

Die AV-Werte generiert das AuC mithilfe der Algorithmen f1 bis f5, jeweils einer nicht vorhersagbaren 128 Bit Zufallszahl, einer teilnehmerspezifischen, aufsteigenden Sequenznummer, dem geteilten Geheimnis K (128 Bit Identitätsschlüssel) und dem AMF-Wert.

Der in Abbildung 13 dargestellte Authentisierungs-Vorgang ist das Gegenstück, welches auf der USIM ausgeführt wird. Dazu empfängt das Mobiltelefon über die Luftschnittstelle die beiden Parameter RAND und AUTN aus einem AV_i, die unverschlüsselt übertragen werden.

Abbildung 13: Authentisierung in der USIM



Im ersten Schritt berechnet USIM mittels f5, K und RAND den Authentication Key (AK). Mit AK kann dann die SQN ermittelt werden. Ist die SQN größer als die zuletzt verwendete und im USIM abgespeicherte SQN_{MS}, wird die SQN gespeichert und die Authentisierung wird fortgesetzt. Entspricht die erhaltene SQN nicht dem Kriterium, wird eine Synchronisations-Fehler-Nachricht zurück an das VLR/SGSN gesendet, welches dann wiederum neue AVs anfordert und der Prozess von neuem beginnt. Nach akzeptierter SQN wird über den Algorithmus f1 der Expected Message Authentication Code (XMAC) ermittelt und mit dem MAC, der im AUTN enthalten war, verglichen. Sind die beiden Werte identisch, gilt der Mobilfunkbetreiber als authentifiziert. Zuletzt erfolgt die Berechnung der RES und den beiden Verschlüsselungswerten CK und IK. Die RES wird in einer „user authentication response"-Nachricht zurück ans VLR übermittelt. Ist die gesendete RES identisch mit der XRES im $A\text{-}V_i$, gilt der Mobilfunkteilnehmer als authentifiziert.

Obwohl die SQN nicht im direkten Zusammenhang mit den beiden Schlüsseln IK und CK steht, sichert die Überprüfung der SQN indirekt unbenutzte Schlüssel zu. Indirekt in dem Sinn, dass dem Netzbetreiber vertraut wird, dass die Zufallszahl RAND vorher nicht schon verwendet wurde, da RAND und SQN in die Berechnung der MAC einfließen.

Unversehrte Schlüssel sind Grundvoraussetzung für eine intakte Verschlüsselung bzw. für den Integritätsschutz. Die Verschlüsselung der Daten und Signalisierungsinformationen erfolgt mit den Algorithmus f8. Dieser ähnelt dem bei GSM verwendeten Algorithmus A5/3, der ebenfalls auf KASUMI basiert. KASUMI ist ein 64-Bit-Blockverschlüsselungsalgorithmus mit einem 128-Bit-Schlüssel, der als ausreichend sicher angesehen wird. Der Algorithmus f9, der für die Datenintegrität verantwortlich ist, basiert ebenfalls auf KASUMI. Mit f9 lässt sich feststellen, ob die Integrität der über die Funkschnittstelle gesendeten Signalisierungsdaten gewährleistet ist. Die Schlüssel IK und CK werden nicht für die gesamte Verbindungsdauer verwendet. Ihr Einsatz (Key Refresh) richtet sich dem Volumen der verschlüsselten Daten und nach einem bestimmten Verwendungsintervall.

Ein wesentlicher Unterschied bei UMTS im Vergleich zu GSM ist, dass die Verschlüsselung zwingend ist und dass zwischen MS und RNC verschlüsselt wird und nicht wie bei GSM nur zwischen MS und BTS (bzw. UMTS äquivalent Node-B). Dies ist eine Folge aus der meist ungesicherten Anbindung über Funkstrecken der Node-B ans RNC.

3.2.2 Schutz der Privatsphäre

Zur Sicherung der Identität eines Benutzers wird nach erfolgter gegenseitiger Authentifizierung mit dem Mobilfunkbetreiber nicht mehr die tatsächliche International Mobile Subscriber Identity (IMSI) sondern die verschlüsselt übertragene Extended Encrypted Mobile Subscriber Identity (XEMSI) verwendet. Diese setzt sich aus der Adresse des zuständigen Netzknotens und der verschlüsselten IMSI, der sogenannten Encrypted Mobile Subscriber Identification (EMSI) zusammen. Die EMSI wird im Betreibernetz unter Zugriff auf das HLR zur ursprünglichen TMSI des Teilnehmers aufgelöst. Hieraus wird die Temporary Encrypted Mobile Subscriber Identity (TEMSI) generiert, welche nun als Sitzungsschlüssel für die weitere Kommunikation mit dem Teilnehmer dient. Um sicher zu stellen, dass ein Benutzer nicht verfolgt werden kann bzw. auch die durch ihn genutzten Dienste nicht zugeordnet werden können, wird die XEMSI periodisch gewechselt und die TEMSI nach jeder Transaktion erneut generiert.

3.3 Sicherheitsgefährdungen

G.13 Abhören von Telefonaten durch Zugriff auf Providernetz

Solche Fälle von Abhörangriffen durch Innentäter bei Mobilfunkbetreibern sind im Falle von GSM bereits dokumentiert. Für UMTS-Netze wären sie bei uneingeschränktem Zugriff auf das Providernetz ebenfalls denkbar.

Schutzmaßnahmen siehe M.14

G.14 Missbrauch von Standard-Leistungsmerkmalen

Die Leistungsmerkmale eines GSM-Netzes können auf vielfältige Weise missbraucht werden. Möglich ist z. B. das Abhören von Raumgesprächen (siehe dazu Kapitel 6).

Gegen den Missbrauch von Standard-Leistungsmerkmalen existieren keine geeigneten Schutzmaßnahmen außer der Abschaltung des Endgeräts (Schutzmaßnahme M.16)

G.15 Erstellung von Bewegungsprofilen durch Ortung

Eine detaillierte Beschreibung der Ortungsmöglichkeiten ist im Kapitel 13.1.1 enthalten. Die Ortung ist im Vergleich zu GSM-Netzen deutlich erschwert, da anstelle der statischen IMSI die dynamischen XEMSI und TEMSI zum Einsatz kommen.

Schutzmaßnahmen siehe M.15, M.16

G.16 Unterbindung von Mobilfunkkommunikation

Mithilfe von Störsendern (englisch jammer) lässt sich sämtliche Kommunikation mit mobilen Endgeräten wirksam unterbinden. Das kommt einer Denial-of-Service-Attacke (DoS-Attacke) gleich. Der Einsatz von aktiven Störsendern ist in Deutschland zumeist verboten. In einigen Bundesländern ist mittlerweile der Einsatz z. B. in Gefängnissen erlaubt, jedoch nur unter strengen Rahmenbedingungen. De facto sind solche Geräte jedoch erwerbbar und kommen auch nachweislich immer wieder zum Einsatz.

Keine geeigneten Schutzmaßnahmen möglich.

G.17 Software-Manipulation

Durch Software-Manipulation oder Modifikation der Software in den mobilen Geräten, lässt sich die Kommunikation auf viele Arten kompromittieren (Firmware, Programme, Viren usw., siehe Kapitel 16).

Schutzmaßnahmen siehe M.88 bis M.95

G.18 Mobiltelefon als Abhörgerät

Durch Manipulation der Endgeräte-Hard- und Software lässt sich ein Mobiltelefon als Abhöreinrichtung missbrauchen (Einbau von Abhöreinrichtungen, Akku mit integrierter Mobilstation usw., siehe Kapitel 14).

Schutzmaßnahmen siehe M.16

G.19 Vorratsdatenspeicherung

Erstellung von Benutzer- und Bewegungsprofilen sowie Rekonstruktion von sozialen Netzwerken auf Grundlage der Vorratsdatenspeicherung.

Schutzmaßnahmen siehe M.13, M.22

G.20 Man-in-the-Middle-Attacke

IMSI-Catcher funktionieren unter Verwendung von UMTS eigentlich nicht, da sich in UMTS-Netzen auch der Betreiber gegenüber dem Endgerät authentisieren muss (gegenseitiges Challenge-Response-Verfahren). Da aus Gründen der geforderten Abwärtskompatibilität allerdings ein Fallback auf GSM unterstützt wird, kann der in Kapitel 1.3.1 beschriebene IMSI-Catcher doch wieder zum Einsatz kommen (siehe [MeWe04]).

Schutzmaßnahmen siehe M.13, M.14

3.4 Mögliche Schutzmaßnahmen

M.13 Sicherheitsanzeige

Verwendung von Mobiltelefonen mit Warnfunktion bei unverschlüsselter Verbindung, beispielsweise je nach Hersteller durch ein offenes Schloss-Symbol am oberen Bildschirmrand dargestellt

M.14 (Sprach-)Datenverschlüsselung

Verwendung von vertrauenswürdigen Crypto-Mobiltelefonen, Crypto-Sprach-Ein-Ausgabemodulen (Hardware) oder Crypto-Software zum Aufbau einer Ende-zu-Ende-Verschlüsselung

M.15 Verschleierung der Identität gegenüber dem Mobilfunkbetreiber

Häufiges Wechseln des Mobiltelefons inklusive SIM-Karte hilft, die eigene Identität zumindest temporär gegenüber dem Dienstanbieter oder eventuellen Angreifern zu verschleiern. Es senkt die Gefahr, dass benutzerspezifische Daten wie etwa die IMSI einem Nutzer eindeutig zugeordnet werden können. Dieses Vorgehen wird erschwert, wenn zum Schutz vor Diebstahl das Endgerät auf die Verwendung mit einer einzigen SIM-Karte eingeschränkt wird (siehe M.7). Darüber hinaus besteht die Gefahr, dass bei Weitergabe von Endgeräten oder SIM-Karten, ob nun unter den Mitarbeitern eines Unternehmens oder sogar über Tauschbörsen, persönliche Daten in unbefugte Hände gelangen (siehe G.67). Hier muss also eine Abwägung getroffen werden, ob die Verschleierung der Nutzeridentität oder die Datensicherheit priorisiert wird.

M.16 Ausschalten des Mobiltelefons und gegebenenfalls Entnahme des Akkus

Da einfaches Drücken des Ausschalters bei einigen Geräten nicht den Mobilfunkteil deaktiviert, muss zur Sicherheit zusätzlich der Akku entfernt werden.

Ausnahme: Es gibt in Akkus integrierte Mobiltelefone zu Abhörzwecken. Dieser Sonderfall ist hierdurch nicht abgedeckt. Weitere Informationen hierzu siehe Kapitel 14.

M.17 Aufbewahrung

Die sichere Aufbewahrung des Endgeräts und insbesondere der SIM-Karte ist die wirksamste Maßnahme gegen Missbrauch der digitalen Identität eines Anwenders und gegen die Kompromittierung des Endgeräts.

M.18 SIM-Karten-Sperrung

Abhanden gekommene SIM-Karten sollten umgehend gesperrt werden. Die SIM-Karte stellt die digitale Identität des Anwenders dar. Da das Kopieren von SIM-Karten denkbar ist (SIM-Cloning, definitiv nachgewiesen für SIM-Karten bis zum Jahr 1999), ist auch nach Wiederfinden der zeitweise verlorenen SIM-Karte eine Kompromittierung denkbar. Eine sofortige Sperrung der SIM-Karte nach Bemerken des Verlusts ist immer zu empfehlen, z. B. über die Hotline des Anbieters.

Eine Möglichkeit, die im Zuge von UMTS bereits teilweise eingeführten UICC zu clonen, und somit Zugriff auf USIM und andere darauf enthaltene Schlüssel zu er-

langen, ist bislang nicht bekannt. Dennoch empfiehlt sich, auch mit diesen Karten wie oben beschrieben zu verfahren.

M.19 SIM-Lock

Viele Endgeräte können auf die Verwendung mit einer einzigen SIM-Karte beschränkt werden. Diese Maßnahme wird meist von Mobilfunk-Anbietern zur Sperrung vertragsgebundener Endgeräte eingesetzt. Hierdurch kann aber auch das Auslesen personenbezogener Daten unter Verwendung einer fremden SIM-Karte unterbunden werden. Dies ist allerdings nur in Verbindung mit der Verschlüsselung der auf dem Endgerät gespeicherten Daten wirksam (siehe M.77).

M.20 Mobiltelefonverbote

Die Mitnahme von Mobiltelefonen in Räumlichkeiten, in denen Gespräche mit vertraulichem Inhalt geführt werden, sollte unterbunden werden. Eine entsprechende Kontrolle ist aufwendig und damit kostenintensiv, sollte aber zum Schutz vertraulicher Daten in Räumen mit erhöhtem Sicherheitsbedarf eingeführt werden.

M.21 Mobilfunkdetektoren

Einsatz passiver Warngeräte (GSM-Mobiltelefon-Detektoren) zur Aufspürung unerwünschter Mobiltelefone. Ein entsprechendes Gerät wird beispielsweise vom BSI vertrieben (siehe [BSIMDS]). Aktive Geräte und Störsender sind in Deutschland nicht zugelassen.

Das Handy ist aktiv und der gesendete Burst kann erkannt werden, sobald Daten gesendet werden, zum Beispiel beim Anmelden, beim Abmelden, wenn Gespräche geführt werde, beim Versenden von SMS, MMS oder beim Webbrowsing. Auf dieser Basis arbeiten Mobilfunkdetektoren, wie zum Beispiel der Mobilfunkdetektor MDS (siehe [BSIMDS]). Dieser Detektor erkennt nur Mobiltelefone im sendenden Betriebszustand und kann so eine Mobilfunkkommunikation (GSM, UMTS und DECT) anzeigen.

Das Betreiben eines aktiven Mobilfunkdetektors, welcher selbst eine Funkzelle nachahmt und so das Telefon zum Senden auffordert, ist nach dem Telekommunikationsgesetz in Deutschland nicht zulässig. Das passive Detektieren hat jedoch den großen Nachteil, dass der Zeitpunkt nicht bestimmt werden kann, zu dem alle Telefone detektiert werden sollen. Ein möglicher Ansatz ist die Ausweitung der Mobilfunkdetektion auf die Location Updates. Damit werden auch Anmeldungen des Mobiltelefons in einer neuen Zelle registriert. Mithilfe eines Verstärkers, eines Transceivers und einer Richtfunkantenne, die das Signal einer weiter entfernten BTS auffängt, kann im lokalen Detektionsbereich das Signalverhältnis so beeinflusst werden, dass sich die Mobiltelefone an der nun stärker sendenden „gefälschten“ Zelle anmelden. Der dabei erfolgende Location Update „enttarnt“ das Mobiltelefon und es wird detektiert. Bei diesem Vorgehen wird die Mobilfunkkommunikation nicht unterbunden, da der Aufbau alle vom Mobiltelefon gesendeten Daten an die entfernte BTS weiterleitet.

M.22 Verwendung von Prepaid-Karten zur Anonymisierung

Ein Kartentausch, der Erwerb von bereits registrierten SIM-Karten oder der Erwerb von Prepaid-SIM-Karten ohne Ausweisprüfung ist zur Vermeidung der Identifikation beim Mobilfunkbetreiber zu empfehlen. Diese Maßnahme verschleiert wirksam die

Identität eines Mobilfunkteilnehmers. Im Geschäftsumfeld kann diese Maßnahme ergänzend für Mobilfunkteilnehmer mit erhöhtem Schutzbedarf durchgeführt werden.

M.23 Benachrichtigung der Überwachungsfunktion

Überwachungsdienstanbieter sind weder per Gesetz noch aus einer Selbstverpflichtung heraus an das Versenden einer Benachrichtigung gebunden. Diese Benachrichtigungs-SMS an das betroffene Endgerät setzt den Anwender über die Überwachung in Kenntnis. Darüber hinaus sollte die Überwachungsfunktion erst nach einer Freischaltung, z. B. durch eine Bestätigungs-SMS an den Diensterbringer, erfolgen.

4. Zukünftige öffentliche Mobilfunknetze

Heutzutage sind Datenübertragungsraten von weniger als 1 Mbit/s kaum ausreichend, um moderne Multimedia-Anwendungen oder auch nur umfangreiche Webseiten zeitnah zu übertragen. Daher haben die Netzbetreiber sehr früh schon damit begonnen, höhere Datenübertragungsraten zu ermöglichen. Seit 2006 verfügen die meisten Netze bereits über den High Speed Downlink Packet Access (HSDPA), um die Datenübertragung zum Endgerät erheblich zu beschleunigen. Weitere Übertragungsverfahren, wie der High Speed Uplink Packet Access (HSUPA) oder der High Speed OFDM Packet Access (HSOPA, OFDM: Orthogonal Frequency Division Multiplexing) versprechen weitere Fortschritte im Hinblick auf den Uplink vom Endgerät zum Festnetz. Ein Ende dieser Entwicklungen ist noch nicht abzusehen und wird zur schrittweisen Einführung von Mobilfunknetzen der vierten Generation führen.

4.1 Technische Grundlagen

Die Verbesserung der Datenübertragungsraten beruht im Wesentlichen auf der Nutzung neuer Multiplexingverfahren, verbesserter Modulation und der optimierten Codierung der Daten. Die dazu verwendeten Verfahren wurden teilweise bereits spezifiziert und werden nun schrittweise von den Providern eingeführt. Während Techniken wie HSDPA und HSUPA bereits Teil des aktuellen Release 6 für UMTS-Netze ist, sind andere noch in der Erprobungsphase. Darunter fällt zum Beispiel HSOPA (High Speed OFDM Packet Access), das in den Standard Long Term Evolution (LTE) aufging und der möglicher Nachfolger von UMTS sein kann.

4.1.1 High Speed Downlink Packet Access

Nahezu alle Mobilfunk-Netzbetreiber bieten High Speed Downlink Packet Access (HSDPA) für deutlich höhere Datenraten im Downlink an. HSDPA ist Teil des Release 6 von UMTS. Unter optimalen Bedingungen ist damit eine theoretische Datenübertragungsrate von 14,4 Mbit/s brutto möglich. Nach Codierung würden davon ca. 10,8 Mbit/s Nettodatenrate bleiben. Die praktisch erreichbare Datenrate ist jedoch aufgrund von notwendigen Fehlerkorrektur-Verfahren und der auf der Luftschnittstelle durch Interferenzen verursachten Störungen deutlich niedriger und beträgt zwischen 1,4 Mbit/s und 5,1 Mbit/s für den Downlink.

HSDPA basiert vollständig auf der oben beschriebenen UMTS-Infrastruktur. Alternativ zu dem gebräuchlichen Quadrature Phase Shift Keying (QPSK) kann als Modulationsverfahren Quadrature Amplitude Modulation (16-QAM) zum Einsatz kommen, ein Modulationsverfahren, das vier Bit auf ein Symbol modulieren kann. Dieser Vorgang ist vergleichbar mit dem Einsatz von EDGE in einem GSM-Netz (siehe Kapitel 2.1.3). Des Weiteren kann HSDPA die per W-CDMA (Wideband Code Division Multiple Access, siehe Kapitel 3.1.2) realisierten Datenkanäle bündeln und gleichzeitig nutzen. Dies kann allerdings zur Folge haben, dass ein Client die gesamte Bandbreite für die Datenübertragung einer UMTS Node-B belegt. Weitere Clients besitzen somit keine Möglichkeit zur Datenübertragung. Dieses Extrem resultiert aus der eingeschränkten Anzahl orthogonaler Codes, die für die Datenübertragung zur Verfügung stehen. Die Vergabe der Kanäle an mehrere Endgeräte wird daher von der Node-B dynamisch realisiert. Das Soft-Handover ist für HSDPA-Verbindungen so

allerdings nicht mehr möglich, da eine hohe Anzahl von Kanälen nicht effizient zwischen den Node-B umziehen kann.

Die erzielbare Datenrate hängt auch vom verwendeten Endgerät ab. Wie auch bei GPRS wurden verschiedene Geräteklassen definiert. Diese geben Auskunft über die unterstützte Modulation (QPSK oder 16-QAM), die Anzahl der gleichzeitig empfangbaren Kanäle und den zeitlichen Mindestabstand von HSDPA-Blöcken. Die ersten kommerziell verfügbaren Geräte erlauben eine Übertragungsrate von bis zu 1,8 Mbit/s (HSDPA-Category 12) oder 3,6 Mbit/s (HSDPA-Category 6). Zukünftige Geräte der HSDPA-Category 8 erlauben eine Datenübertragungsrate von maximal 7,2 Mbit/s.

4.1.2 High Speed Uplink Packet Access

Mit dem Aufbau des High Speed Uplink Packet Access (HSUPA) soll die maximal verfügbare Datenrate vom Endgerät zum Festnetz (Uplink) zunächst auf 1,4 Mbit/s und später dann auf 5,8 Mbit/s gesteigert werden. HSUPA ist wie HSDPA Teil des Release 6 von UMTS und gehört zur sogenannten Generation 3,5 (3.5G) der Mobilfunknetze, befindet sich aber noch in der Entwicklungs- und Erprobungsphase. Erste Ausbauten sollen im Jahr 2008 abgeschlossen werden. Als Modulationsverfahren wird aller Voraussicht nach 16-QAM zum Einsatz kommen.

4.1.3 High Speed OFDM Packet Access

Die nächste Ausbaustufe ist nach der derzeitigen Planung die Einführung von High Speed OFDM Packet Access (HSOPA) im Rahmen der sogenannten Next Generation Mobile Networks (NGMN) bis zum Jahre 2010. Damit zeichnet sich schon die nächste Generation der Mobilfunknetze ab, die auch als Long Term Evolution (LTE) oder als Super 3G bezeichnet wird.

Mit Orthogonal Frequency Division Multiplexing (OFDM) wird das verwendete Multiplexingverfahren auf der Luftschnittstelle bezeichnet. OFDM nutzt im Gegensatz zu W-CDMA kein Code-Multiplexing, sondern eine besondere Form des Frequenzmultiplexings. Hierzu werden die Daten parallel über eine Vielzahl von Frequenzkanälen übertragen, statt zwischen diesen Kanälen zu springen. Zwar geht hierdurch der Vorteil der Störfestigkeit zunächst scheinbar verloren. Betrachtet man aber die in dieser Technik mögliche längere Symboldauer, so erhöht sie sich im Gegenteil sogar. Mithilfe von HSOPA sollen noch deutlich höhere Datenübertragungsraten zu erzielen sein, als es mit HSDPA und HSUPA denkbar ist. Derzeit werden daher Übertragungsraten von ca. 100 Mbit/s im Downlink und 50 Mbit/s im Uplink erwartet. OFDM-basierte Netze werden auch als 3.9G bezeichnet.

4.1.4 Mobilfunksysteme der vierten Generation

Nach der stufenweisen Einführung der bis dato entwickelten Übertragungstechnologien, zeichnen sich heute verschiedene Technologien als mögliche Mobilfunksysteme der vierten Generation ab. Darunter fällt das 3GPP LTE (Third Generation Partnership Project Long Term Evolution), welches versucht, aufbauend auf den heutigen UMTS-Mobilfunkstandards, zukünftige Anforderungen an das Mobilfunknetz zu erfüllen. Ein weiterer Ansatz sind

WLANs nach 802.11n, welche im Kurzstreckenbereich eingesetzt werden können und Bruttodatenraten bis 600 Mbit/s erlauben werden[2]. Die Reichweiten erhöhen sich im Vergleich zum Standard 802.11g ebenfalls. Für den Einsatz in größeren Entfernungen zur Basisstation könnte sich WiMAX als interessantes Medium erweisen, ein Synonym für die drahtlosen Netzwerkstandards der 802.16-Familie. Insbesondere ist hier der Standard 802.16e, der das Roaming zwischen Basisstationen erlaubt, interessant. In direkter Nachfolge zu diesem bereits spezifizierten Standard soll 802.16m stehen. Dieser wird momentan entwickelt und soll Datenraten von bis zu 1 Gbit/s für sich langsam bewegende Teilnehmer im Nahbereich und bis 100 Mbit/s für schnell bewegte Teilnehmer im Fernbereich ermöglichen. Der Standard würde als erster aus der WLAN-Familie alle für den Aufbau eines 4th Generation Network (4G) erforderlichen Eigenschaften mitbringen.

Welche Funktechnologie aber auch an der Schnittstelle zum mobilen Endgerät eingesetzt wird, die Forderungen an ein Mobilfunknetz der Zukunft sind klar. Im Zuge der Verschmelzung von Fest- und Mobilnetzen zu Next Generation Networks (NGN) werden auch die Next Generation Mobile Networks (NGMN) in ihrem Kern immer stärker auf IP basieren. Ziel muss es sein, dass die genutzten Daten- und Kommunikationsdienste – unabhängig von den zugrunde liegenden Medien – für den Anwender transparent im gesamten Netz verfügbar werden. Daher werden 4G Netze aller Voraussicht nach auf einer gemeinsamen IP-gestützten Plattform aufsetzen.

Das hätte neben den möglichen Vereinfachungen der Netzinfrastruktur auch einige praktische Vorteile. So wäre ein Handover von Diensten nicht nur zwischen Funkzellen eines Mobilfunk-Anbieters möglich. Denkbar wäre auch ein Handover einer Dienstsitzung von Provider zu Provider, von Medium zu Medium und auch über Landesgrenzen hinweg. So wäre auch ein weltweit identisches Angebot von Dienstmerkmalen durch Provider realisierbar, was für Kunden und Provider gleichermaßen Vorteile bietet.

Jedoch stellen diese Visionen auch einige Herausforderungen an die technische Umsetzung. Die Konvergenz der Providernetze und der Client-Anbindung hin zu IP-basierter Datenkommunikation trägt die Sicherheits-Probleme der IP-basierten Festnetze in die Mobilfunknetze hinein. Daher ist es notwendig, diese 4G-Netze von vornherein unter der Berücksichtigung solcher Sicherheitsaspekte zu entwickeln. Als Beispiel sei die Pass Through Authentication genannt, die eine Authentifizierung über Providergrenzen hinweg ermöglichen soll. Ein weiterer Aspekt wäre das Roaming von Ende-zu-Ende-verschlüsselten Dienstsitzungen zwischen Providern. Die bislang empfohlenen Implementierungen von Sicherheitsmerkmalen können auf lange Sicht den wachsenden Anforderungen nach Sicherheit nicht gerecht werden, weshalb ein global gültiger Sicherheitsstandard für 4G-Netze als kleinster gemeinsamer Nenner immer notwendiger wird. Die Herausforderung ist es, diesen qualitativ hoch genug anzusetzen, um den wachsenden Sicherheitsbedürfnissen von Kunden und Providern gerecht zu werden.

4.2 Sicherheitsgefährdungen

Im Folgenden wird lediglich auf die Sicherheitsgefährdungen eingegangen, die zusätzlich zu den mit UMTS bereits bekannten existieren.

[2] Aktuelle Vorstandard-Produkte unterstützen bis zu 300 MBit/s.

4.2.1 HSDPA und HSUPA

HSDPA und HSUPA sind Übertragungsdienste ohne eigene Methoden zur Authentisierung oder Verschlüsselung. Diese Mechanismen sind mit denen im UMTS-Netz identisch und somit kommen aus dieser Sicht keine zusätzlichen Gefährdungen hinzu.

Zusätzliche Gefährdungen entstehen allerdings durch die Tatsache, dass hier breitbandige Datenverbindungen aufgebaut und weitere Dienste genutzt werden (z. B. WAP (Wireless Application Protocol), Internetapplikationen usw.). Die entsprechenden Dienste und ihrer Gefährdungen werden in Kapitel 8 beschrieben.

Die Nutzung von Datendiensten mit großen Übertragungsraten ist allerdings momentan auf Grund der hohen Aktivierungskosten von Seiten der Provider relativ teuer. Daher sind die, teilweise immensen, Kosten, welche unter geeigneten Bedingungen entstehen können, noch als „Gefährdung“ zu nennen. Falls kein entsprechender Volumen- oder Zeittarif abgeschlossen wird, entstehen Datenvolumengebühren. Es sind Fälle bekannt, in denen z. B. 96,00 Euro für den Download von zwei (!) Mails mit je ca. 1 MB Anhang entstanden sind. Auch die Roaming-Gebühren sind bei UMTS noch nicht vollkommen transparent und können aufgrund der verhältnismäßig hohen Geschwindigkeiten der Dienste schnell zu hohen Kosten führen.

4.2.2 HSOPA

HSOPA wird als Nachfolger von UMTS mindestens abwärtskompatibel mit UMTS und eventuell sogar mit GSM sein. Prinzipiell ist daher zu vermuten, dass die zugrunde liegenden Schutzmechanismen lediglich erweitert und dann optional geboten werden.

[NGMN06] fordert hier für ein solches Netz:

- **“Recommendation:** Supports highest level of security for users, network elements, devices, and service enabling platforms.“[3]
- “NGMN shall support lawful interception as an inherent part of the network to exploit functional synergies.”[4]
- “It should be possible for Operator-provided services to provide end-to-end security for user plane traffic with a key escrow mechanism (to enable lawful-interception of end-to-end traffic if required)”[5]

Die Datendienste auf Basis von HSOPA unterliegen keinen zusätzlichen Gefährdungen durch die verwendete Übertragungstechnologie. Aufgrund der höheren Datenübertragungsraten ent-

[3] „Empfehlung: Bietet den höchsten Grad an Sicherheit für Anwender, Netzelemente, Endgeräte und Dienste ermöglichende Plattformen.“

[4] „Das NGMN muss zur Nutzung von funktionale Synergien eine gesetzlich autorisierte Überwachung (englisch Lawful Interception) als System-immanenten Teil des Netzs unterstützen.“

[5] „Es sollte für von Netzanbietern gebotene Dienste möglich sein, Ende-zu-Ende Sicherheit für den Datenverkehr auf Anwenderebene unter Verwendung eines Schlüssel-Hinterlegungs-Mechanismus anzubieten (um Lawful Interception für Ende-zu-Ende verschlüsselten Datenverkehr zu ermöglichen).“

stehen jedoch auch ähnliche Gefahren wie in Kapitel 2.2.2 dargestellt. Gefährdungen, die aufgrund von Dienstnutzung entstehen, werden in Kapitel 8 erläutert.

4.3 Mögliche Schutzmaßnahmen

Wie in Kapitel 4.2 beschrieben werden Schutzmaßnahmen unter den jeweiligen weiteren Diensten genannt (siehe Kapitel 8 und 12).

5. Satellitengestützte Mobilfunknetze

Es existiert eine Reihe satellitengestützter Kommunikationsnetze. Darin werden Daten und Sprache direkt vom Endgerät an einen Satelliten gesendet, von wo aus diese an einen anderen Teilnehmer im Satellitennetz oder auch in ein anderes Kommunikationsnetz weitergeleitet werden. Die Sprach- und Datenkommunikation via Satellit bietet eine Reihe von Vorteilen. So ist zum Beispiel eine lokale Netzinfrastruktur bestehend aus einer Vielzahl von Funkzellen mit verhältnismäßig kurzer Reichweite nicht erforderlich.

Die sogenannte Ausleuchtzone (englisch footprint), also das von Funksender und Funkempfänger des Satelliten ausgeleuchtete Gebiet, kann durchaus – abhängig von der verwendeten Technologie – mehrere tausend Kilometer betragen. Dadurch wird eine deutlich höhere Abdeckung erreicht, als beispielsweise mittels GSM. Vor allem in der Luftfahrt, dem maritimen Bereich und in dünn besiedelten Gebieten wird gerne auf diese Technik zurückgegriffen. Nachteil sind die aufgrund der aufwendigen Technologie hohen Verbindungskosten, die hohen Kosten für Endgeräte sowie der mangelhafte Empfang innerhalb von Gebäuden und bei schlechten Wetterverhältnissen. Für die Kommunikation per Satellit gelten einige Einschränkungen. So ist der Einsatz von Endgeräten für Satellitennetze nicht weltweit erlaubt (in der Regel aus politischen Gründen, z. B. teilweise in Osteuropa und Asien verboten). Einige technische Details satellitengestützter Kommunikationsnetze werden im Folgenden beschrieben.

5.1 Technische Grundlagen

Der herkömmliche Aufbau satellitengestützter Netze basiert auf geostationären Satelliten, also Satelliten, die ihre Position relativ zur Erdoberfläche beibehalten. Dieses Konzept namens Geostationary Earth Orbiting (GEO) erfordert die Positionierung der Satelliten in großen Höhen, da die Geschwindigkeit der Satelliten auf ihrer Umlaufbahn hoch sein muss, um der Erdanziehung entgegenzuwirken. Vorteil ist die gezielte Abdeckung bestimmter Gebiete der Erdoberfläche. Nachteile ergeben sich aus den großen erforderlichen Höhen, die lange Übertragungswege und damit hohe Latenzen in Sprach- und Datenverbindungen hervorrufen. Außerdem ist auf Endgeräteseite in der Regel eine aufwendigere Technik wie z. B. Richtfunkantennen und eine höhere Sendeleistung erforderlich, um die hohen Distanzen zu den Satelliten zu überwinden.

Low Earth Orbiting (LEO) hingegen bezeichnet niedrig positionierte Kommunikationssatelliten in Höhen von einigen hundert Kilometern. Sie bewegen sich mit der zur Beibehaltung ihrer Höhe notwendigen Geschwindigkeit auf einer kreis- oder ellipsenförmigen Bahn. Die niedrige Positionierung ermöglicht deutlich geringere Latenzen als im Fall von GEO-Satelliten. Auch der resultierende geringere Abstand zwischen einzelnen Satelliten eines Netzes trägt hierzu bei. Da LEO-Satelliten relativ zum Mobilfunkteilnehmer auf der Erde bewegt sind, müssen bestehende Verbindungen häufig zwischen Satelliten übergeben werden. Hierzu unterstützen LEO-basierte Kommunikationsnetze Seamless Handover, also die Übergabe ohne Beeinträchtigung der Verbindung. Diese Technik wird auch dazu verwendet, Verbindungen von Benutzern, die sich in den Funkschatten von Gebirgen oder Gebäuden begeben, auf einen anderen Satelliten zu übergeben und die Datenverbindung dennoch beizubehalten.

5.1.1 Netz und Routing

Die Satelliten bilden in einem satellitengestützten Netz oft nur die Schnittstelle zwischen mobilen Endgeräten und einem Netz von Bodenstationen. Häufig werden Daten und Sprache vom Satelliten an eine Bodenstation gesendet, von der aus diese dann an den Empfänger weitergeleitet werden. Dies kann auch über ein bodengebundenes Netz stattfinden. Befindet sich der zweite Teilnehmer im selben Satellitennetz, so findet eine Weitervermittlung an den für den zweiten Teilnehmer zuständigen Satelliten statt.

Insbesondere bei LEO-Netzen mit einer hohen Anzahl von Satelliten findet ein anderer Ansatz Verwendung. Verbindungen innerhalb des Netzs werden zwischen den Satelliten direkt übertragen. Nur im Falle einer Verbindung über Netzgrenzen hinweg wird eine Bodenstation einbezogen, um die Verbindung über Gateways in andere Netze zu vermitteln. Eine große Anzahl an Satelliten ist hierfür allerdings Voraussetzung, da auch Bandbreite von nicht direkt mit den Endgeräten in Verbindung stehenden Satelliten belegt wird und die Bandbreite pro Satellit begrenzt ist.

5.1.2 Kommunikation

Für die Nutzung durch kommerzielle Kommunikationssatelliten steht eine Reihe von Frequenzbändern zur Verfügung, die von der International Telecommunication Union (ITU) für diese Nutzung reserviert wurden. L- und S-Band im Bereich von 1,5 bis 2,2 GHz werden teilweise bereits durch andere, erdgebundene Technologien verwendet und stehen daher nur eingeschränkt zur Verfügung. Hinzu kommt die relativ niedrige Bandbreite von 15 bzw. 75 MHz, die die Zahl der gleichzeitig nutzbaren Funkkanäle deutliche beschränkt. Die in höheren Frequenzbereichen angesiedelten C- und Ku-Bänder bieten deutlich höhere Bandbreiten von rund 500 MHz. In diesen Mikrowellenbändern ist der erdgebundene Funkverkehr auch deutlich niedriger. Allerdings haben hier Störeffekte durch terrestrische Interferenzen und Umwelteinflüsse wie Regen deutlich stärkere Auswirkungen.

Heutige Satelliten unterteilen die für Senden und Empfangen von Daten zur Verfügung stehende Bandbreite dynamisch in Kanäle. Während ältere Systeme hier in der Regel statisch das Band in Frequenzkanäle unterteilen (Frequency Division Multiplexing, FDM), geschieht die Einteilung heute in Zeitscheiben, die einem Kommunikationspartner zugewiesen werden (Time Division Multiplexing, TDM). Hierdurch wird eine Zahl von mehreren tausend gleichzeitigen Kommunikationskanälen pro Satellit erreicht. Iridium-Satelliten verfügen z. B. über rund 3800 Kanäle mit unterschiedlichen Verwendungszwecken.

Die bei der Satellitenkommunikation zur Verfügung stehenden Datenraten variieren sehr stark nach Art des Satelliten und seines Einsatzzwecks. Prinzipiell lassen sich mit Satelliten, welche in einem höheren Frequenzband agieren, auch höhere Datenraten erzielen. Der Einsatzzweck ist ebenfalls ausschlaggebend; während reine Telefonprovider ihre Datenraten pro Kanal stark beschränken, um eine höhere Anzahl gleichzeitiger Nutzer zu versorgen, erlauben Datendienstanbieter eine höhere Bandbreite. Technisch sind extrem hohe Bandbreiten möglich, wie die Planung des Teledesic-System belegt. Vorgesehen waren hier Kanäle mit 100 Mbit/s Upstream und 720 Mbit/s Downstream. Dass die Entwicklung dieses Systems trotzdem 2002 eingestellt wurde, lag nicht an der technischen Realisierbarkeit sondern an der kommerziellen Verwertbarkeit des Satellitendienstes. Durchschnittliche Datenraten heute verfügbarer Satellitenservices liegen zwischen 9,6 kbit/s und 2 Mbit/s.

5.1.3 Dienste

Es wird eine Vielzahl von Diensten in Satellitennetzen angeboten. Die Sprachkommunikation, die mit unterschiedlichen Datenraten zwischen 2,4 kbit/s und 64 kbit/s angeboten wird, basiert in der Regel auf GSM-ähnlicher Technologie. Auch SMS-ähnliche Dienste werden geboten, etwa das bei Inmarsat verwendete Messaging-Format, das den Versand von bis zu 32.000 Zeichen (7-Bit-Zeichen), also ca. 28 KByte großer Nachrichten ermöglicht. Eine Zustellung an den Empfänger per E-Mail wird von Inmarsat ebenfalls angeboten.

Zur Datenübertragung kommen oft GPRS-ähnliche Dienste zum Einsatz, etwa der Mobile Packet Data Service (MPDS), der 64 kbit/s Datenraten ermöglicht. Mit der zunehmenden Nutzung von Breitband-Applikationen steigt der Bedarf nach entsprechenden Übertragungswegen via Satellit. Hier kommen Satellitendienste wie Broadband Global Area Network (BGAN) bzw. Regional BGAN (RBGAN) zum Einsatz, die eine Bandbreite von 128 kbit/s garantieren, aber auch höhere Datenraten bis zu 2 Mbit/s erlauben.

Neben diesen aus den terrestrischen Fest- und Mobilfunknetzen bekannten Diensten bieten Satellitennetze einige spezifische Dienste, die ihre Wurzeln beispielsweise im maritimen Einsatz haben. So können in einigen Netzen per Polling Daten eines Teilnehmers abgefragt werden, etwa um die GPS-Daten eines Schiffes abzufragen. Data Reporting stellt ein automatisiertes Polling dar. Gruppenrufe sind ebenfalls häufig möglich, bei Inmarsat werden diese z. B. für die Distribution von Sturmwarnungen genutzt. Auch priorisiertes Routing stammt aus dem maritimen Bereich, wurde es doch ursprünglich zum Versand von Schiffsnotrufen in Satellitennetzen eingeführt.

5.1.4 Beispiele für Satelliten-basierte Kommunikationssysteme

- Inmarsat basiert auf momentan elf GEO-Satelliten, die in einer Höhe von ca. 35.800 Kilometern über der Erdoberfläche stationiert sind. Es wurde ursprünglich für die Satellitenkommunikation im Hochseeverkehr aufgebaut und bietet heute darüber hinaus kommerzielle Sprach- und Datendienste an. Auch für den Luftverkehr werden Dienste angeboten. Trotz geostationärer Bahnen wird, abgesehen von den nicht ausgeleuchteten Polkappen, eine großflächige Abdeckung erreicht. Details zu Inmarsat und den angebotenen Diensten finden sich auf der Inmarsat Website (siehe [INMS]).

- Iridium ist ein kommerzielles Satellitennetz, welches auf LEO-Satelliten basiert. Die momentan 66 aktiven Satelliten des Iridiumnetzs befinden sich in Nähe zu den Erdpolen im Orbit. In einer Höhe von rund 780 Kilometern bewegen sie sich in Formationen à 11 Satelliten mit untereinander konstanten Abständen. Sie sind in Gruppen untereinander vernetzt, wobei jeder Satellit Verbindung zu zwei Satelliten derselben Formation und zu zwei weiteren in jeweils anderen Formationen aufrecht erhält. Dadurch ergibt sich ein mehrfach vermaschtes, in sich geschlossenes Netz, das Ausfälle von Satelliten und Bodenstationen kompensieren kann. Das Iridium-Netz verzichtet beim Routing von Verbindungen zwischen zwei Teilnehmern des Satellitennetzs größtenteils auf Umwege über Bodenstationen. Lediglich bei Verbindungen in andere Netze werden die Daten über Bodenstationen geleitet, welche die Anbindung zu anderen Netzen durch Gateways ermöglichen. Weitere Details finden sich auf der Betreiberwebseite (siehe [IRID]).

- Globalstar bietet – wie Iridium auch – Sprach- und Datendienste. Es basiert auf 40 LEO-Satelliten, die die Erde auf überkreuzenden Bahnen in einer Höhe 1.414 Kilometern um-

kreisen. Die Betreiber geben an, hierdurch eine Abdeckung von 80% der Erdoberfläche zu erreichen. Hinzu kommen vier Satelliten als Sicherung gegen technische Ausfälle. Handover ist bei Globalstar durch ein redundantes Konzept gelöst. Mehrere Satelliten nehmen gleichzeitig die Verbindung an und halten diese aufrecht. Verliert nun das Endgerät den Kontakt zu einem dieser Satelliten, bricht die Verbindung nicht zusammen, da die Verbindung über einen anderen Satelliten weiterhin besteht. Im Gegensatz zu Iridium residiert die Systemsoftware fast ausschließlich in den Bodenstationen. Das schließt das Routing mit ein, weshalb kein Routing zwischen Satelliten stattfindet. Weitere Informationen finden sich unter [GLST].

- Thuraya ist das Satellitenkommunikationsnetz eines arabischen Netzbetreibers bestehend aus momentan zwei geostationären Satelliten. Die Abdeckung ist dadurch auf den europäischen, afrikanischen und kleinasiatischen Raum beschränkt. Ein dritter Satellit ist in Planung. Interessant ist der variable Abdeckungsbereich, der durch mehrere sogenannte Spot Beams pro Satellit realisiert wird. Deren Ausrichtung lässt sich den aktuellen Anforderungen an die Abdeckung anpassen. Einem mobilen Endgerät wird anhand seiner GPS-Position (Global-Positioning-System-Position) der zuständige Spot Beam zugewiesen (siehe [THUR]).

5.2 Sicherheitsgefährdungen

G.21 Gefährdungen für GSM-Endgeräte

Viele Sprachdienste per Satellit weisen große Ähnlichkeiten zu GSM auf. Daher existiert eine Vielzahl von Endgeräten, die wahlweise satellitengestützte oder GSM-basierte terrestrische Mobilfunknetze nutzen können. Für diese Endgeräte bestehen grundsätzlich dieselben Gefährdungen, die sich aus der Nutzung von GSM ergeben.

Schutzmaßnahmen siehe Kapitel 1.3.3

G.22 Routing über Bodenstationen

Das Routing von Daten innerhalb von Satellitennetzen ist für den Nutzer nicht direkt nachvollziehbar. Abhängig vom Anbieter werden Daten entweder vom Satellit zunächst zur Bodenstation und dann über das Providernetz geroutet oder direkt zwischen Satelliten bis zum Adressaten. Das Routing über Bodenstationen stellt eine potenzielle Sicherheitslücke dar. Ist diese Bodenstation in einem Land mit niedrigsten Datenschutzbestimmungen angesiedelt, so greifen eventuell lokale rechtliche Bestimmungen beim Routing über diese Stationen. Die Integrität der Daten kann also nicht unbedingt gewährleistet werden.

Schutzmaßnahmen siehe M.24, M.25, M.26

G.23 Unklare Datenschutzbestimmungen im All

Auch das Routing von Daten zwischen Satelliten ist eine datenschutzrechtliche Grauzone. Es gibt aktuell keine (internationalen) gesetzlichen Regelungen zu personenbezogenen Daten, die vom Weltraum aus erfasst werden und auch im Weltraum verarbeitet werden. Eine solche Regelung wäre eventuell durch die UN oder das COmmittee on the Peaceful Use of Outer Space (COPUOS) zu erwarten. Hier ist man bislang auf die Integrität des Satellitenproviders angewiesen. Ein mögliches

Abhören der Kommunikation zwischen Satelliten ist zwar technisch möglich, aber aufgrund des extremen technischen Aufwands sehr unwahrscheinlich.

Schutzmaßnahmen siehe M.24, M.26

G.24 Großer Abstrahlbereich

Zitat aus [DSBer20]: „Die via Satellit abgestrahlten Signale sind […] prinzipiell im gesamten Ausstrahlungsbereich (englisch footprint) des benutzten Satelliten von jedermann, der über geeignete technische Einrichtungen verfügt, zu empfangen. Die bei der Übertragung verwendeten Multiplexverfahren bieten nur einen unvollständigen Schutz. Einrichtungen zur Überwachung der Satellitenkommunikation werden in vielen Ländern auch von staatlichen Stellen betrieben, die die gesamte Satellitenkommunikation in ihrem Einzugsbereich abhören und auswerten. Darüber hinaus ist die Existenz gleichartiger privater Einrichtungen – z. B. zum Zweck der Industriespionage – durchaus denkbar."

Schutzmaßnahmen siehe M.24

G.25 Keine klaren Datenschutzregelungen

Zitat aus [DSBer20]: „Wie oben ausgeführt, entstehen durch die verstärkte Nutzung der Satellitentechnik auch zunehmend Gefahren für das informationelle Selbstbestimmungsrecht des Einzelnen, ohne dass bisher umfassende Datenschutz- und Datensicherheitsregelungen zur Eindämmung dieser Gefährdungen entwickelt worden wären. Die Entwicklung der Satellitenkommunikation sollte daher von den Datenschutzbeauftragten stärker als bisher kritisch begleitet werden."

Schutzmaßnahmen siehe M.26

G.26 Störung der Endgerätekommunikation

Die Kommunikation von mobilen Endgeräten mit Satellitennetzen kann durch fest installierte oder transportable Störsender (englisch jammer) unterbunden werden. Für Satellitennetze, die das L-, S- oder C-Band verwenden, ist dies technisch relativ einfach möglich. Entsprechende Geräte, die im niedrigen GHz-Bereich arbeiten, sind, obwohl der Einsatz in Ländern der europäischen Union nur für bestimmte Nutzerkreise (Behörden, Militär) erlaubt ist, weitgehend frei verfügbar. Störsender für Ku- und Ka-Band sind möglich, aber aufgrund der höheren Betriebsfrequenzen technisch aufwendiger und dementsprechend teurer und weniger weitverbreitet.

Keine geeigneten Schutzmaßnahmen möglich.

G.27 Störung des Satellitennetzs

Die Störung ganzer Satellitennetze ist technisch ähnlich realisierbar, wie die Störung der Endgerätekommunikation (G.26). Hierzu müsste die Kommunikation zwischen Bodenstationen und Satellit bzw. zwischen einzelnen Satelliten gestört werden. Die Störung der Kommunikation von Bodenstationen ist deutlich einfacher zu realisieren, setzt aber aufgrund der notwendigen Sendeleistungen auch einen erheblichen technischen Aufwand voraus. Eine Störung der Intersatellitenkommunikation ist wegen des extremen technischen Aufwands – wenn überhaupt – nur von staatlicher bzw. militärischer Seite aus zu realisieren.

Keine geeigneten Schutzmaßnahmen möglich.

5.3 Mögliche Schutzmaßnahmen

M.24 Ende-zu-Ende-Verschlüsselung

Zitat aus [DSBer20]: „Wie bereits oben ausgeführt, kann eine via Satellit übertragene Nachricht im Prinzip im gesamten Abstrahlbereich des Satelliten abgehört werden. Soweit die Dienstanbieter den Benutzern keine wirksame Ende-zu-Ende-Verschlüsselung anbieten, sollten die Benutzer daher – zumindest wenn sensible Daten übertragen werden sollen – selbst derartige Verschlüsselungsverfahren anwenden."

M.25 Rechtliche Absicherung von Verschlüsselungseinsatz

Vor dem Einsatz von Verschlüsselungstechnologie auf mobilen Endgeräten im nicht-europäischen Ausland muss deren Einsatz rechtlich abgesichert werden. Eine Ende-zu-Ende-Verschlüsselung ist, ebenso wie Satellitenkommunikation selbst, nicht überall legal. Kann keine Verschlüsselung eingesetzt werden, so ist auf die Übertragung sensibler Daten vollständig zu verzichten.

M.26 Klärung von Datenschutzbestimmungen

Vor der Nutzung von Satellitennetzen ist eine rechtliche Prüfung der auf den Routingpfaden gültigen Datenschutzbestimmungen empfehlenswert. Falls ein Provider als datenschutzrechtlich kritisch eingestuft werden muss, so sollte – falls möglich – auf einen alternativen Anbieter ausgewichen werden. Eine wirksame Ende-zu-Ende-Verschlüsselung hilft auch hier, persönliche und vertrauliche Informationen bei Routing über unsichere Netze zu schützen.

6. Allgemeine mobile Telefondienste

Die Betreiber von Mobilfunknetzen bieten ihren Kunden eine Reihe von Leistungsmerkmalen an, die über das reine Telefonieren hinausgehen. Solche Leistungsmerkmale können aber unter anderem durch Fehlbedienung infolge Fehlkonfiguration die Verfügbarkeit, Vertraulichkeit und Integrität der mobilen Kommunikation gefährden.

In diesem Kapitel werden beispielhaft für allgemeine mobile Telefondienste die folgenden Themen betrachtet:

- Konferenzschaltung
- Push-to-Talk
- Mehrwertdienste

Nach einer jeweiligen kurzen Einführung werden die wichtigsten Sicherheitsgefährdungen dargestellt sowie, falls vorhanden, entsprechende Gegenmaßnahmen genannt.

6.1 Technische Grundlagen

6.1.1 Konferenzschaltung

Ein Gesprächsaufbau mit mehr als zwei gleichzeitigen Teilnehmern wird als Konferenzschaltung bezeichnet. Das Hinzufügen zusätzlicher Gesprächsteilnehmer kann auf zwei Wegen erfolgen:

1. Der Initiator der Konferenzschaltung lädt zusätzliche Teilnehmer über einen entsprechenden Anruf ein.
2. Ein zusätzlicher Teilnehmer ruft während der laufenden Konferenzschaltung den Initiator an und lässt sich als zusätzlichen Teilnehmer aufnehmen.

Die Durchführung von Konferenzschaltungen muss sowohl vom Netzbetreiber als auch vom Endgerät des Initiators der Konferenzschaltung unterstützt werden. Aus Sicht der anderen Teilnehmer handelt es sich bei der Konferenzschaltung um eine normale Ende-zu-Ende-Verbindung.

6.1.2 Push-to-Talk

Mobiltelefone, welche Push-to-Talk (PTT) unterstützen, können wie eine Wechselsprechanlage genutzt werden. Hierbei wird bei Betätigung einer festgelegten PTT-Taste das nachfolgend Gesprochene an vorkonfigurierbare Empfänger gesendet. Als Empfänger können in der Regel auch Gruppen mit mehreren Mitgliedern ausgewählt werden. Typischerweise findet die Sprachübertragung bei PTT im Semi-Duplex-Verfahren statt. Das heißt, prinzipiell kann jeder Teilnehmer Sprachdaten senden und empfangen; es ist aber immer nur ein Teilnehmer gleichzeitig sendeberechtigt.

Während die ersten Anbieter ihre proprietären PTT-Dienste nur auf Basis bestimmter Hardware anboten, basiert Push-to-Talk heute meist auf VoIP über GPRS. Auch kann es auf dem IP Multimedia Subsystem (IMS) aufsetzen. Neben proprietären Implementierungen dieses Dienstes wurde ein SIP-basiertes (Session Initiation Protocol) Dienstdesign namens PTT over Cellular (PoC) durch die Open Mobile Alliance (OMA) entwickelt. Nach ausführlichen Kompatibilitätstests und Erweiterungen befindet sich nun PoC Version 2 in der Standardisierungsphase.

PoC basiert auf der Kombination von mobilen Datendiensten mit bereits standardisierten VoIP-Protokollen (Voice over IP). Zur Signalisierung wird das Session Initiation Protocol (SIP) verwendet, welches auch in kabelgebundenen Datennetzen zur Signalisierung von VoIP-Sitzungen große Relevanz hat. Die Übertragung der Sprachdaten wird anhand des Real Time Protocol (RTP) realisiert, während die Dienstgüte durch den Einsatz von Real Time Control Protocol (RTCP) sichergestellt wird. Die Spezifikation von PoC beschreibt jedoch nicht die Interoperabilität mit Secure RTP (SRTP), das verschlüsselte Sprachverbindungen erlaubt.

Zur Realisierung der eigentlichen Push-to-Talk-Funktionalität wird das im PoC-Standard festgeschriebene Talk Burst Control Protocol (TBCP) verwendet. Dies ist notwendig, da Sprachdaten im Vergleich zu Telefonaten nicht im Full-Duplex-Modus (beide Senderichtungen zeitgleich), sondern im Semi-Duplex-Modus (nur eine gleichzeitige Senderichtung) übertragen werden. TBCP realisiert hierfür zum Beispiel die Anforderung des Senderechts (TBCP Talk Burst Request) für einen PTT-Client am zentralen PTT-Server.

Durch die Wiederverwendung von offenen, standardisierten Protokollen im PoC-Standard soll eine größtmögliche Interoperabilität von PTT mit bereits existierenden und zukünftigen Sprach- und Datendiensten in Mobilfunknetzen erreicht werden.

6.1.3 Mehrwertdienste

Für den Bereich der Mehrwertdienste existiert keine klare und verbindliche offizielle Definition. Prinzipiell gilt, dass dies Telekommunikationsdienste sind, welche über die rein technische Bereitstellung einer Telekommunikationsverbindung hinausgehen.

Mehrwertdienste werden beispielsweise durch Versenden einer SMS an eine bestimmte Nummer oder aber durch einen Telefonanruf vom Kunden angefordert. Bei Mehrwertdiensten auf Basis von Telefonverbindungen kommt ein Vertragsverhältnis mit entsprechend anfallenden Kosten zustande, sobald eine Mehrwertdienstnummer gewählt wurde und die Verbindung nach erfolgter Preisinformation aufrecht erhalten wird. Telefonische Mehrwertdienste werden im Allgemeinen über 0900-Nummern erbracht.

Darüber hinaus werden Mehrwertdienste angeboten, die bereits bei der Tätigung eines Telefonanrufs (genauer: sofort beim Zustandekommen einer Telefonverbindung) zusätzliche Kosten verursachen. Dies sind beispielsweise Anrufe zu Telefonnummern aus dem 0137er Bereich, welche als MABEZ (Massenverkehr zu bestimmten Zielen) Rufnummern genutzt werden und oft Zwecken wie der Durchführung von Zuschauerabstimmungen dienen.

Weitere Nummernkreise, die beim Anruf erhöhte Kosten verursachen sind Auskunftsnummern 118xy, Shared Cost Nummern 0180x sowie innovative Dienste 012xx.

6.2 Sicherheitsgefährdungen für den Nutzer

6.2.1 Konferenzschaltung

Konferenzschaltungen ermöglichen unter bestimmten Bedingungen ein unbemerktes Abhören von Telefonverbindungen. Ein Teilnehmer einer bestehenden Telefonverbindung kann eine weitere Person anrufen und diese anschließend in eine Konferenz aufnehmen. Die angerufene Person erkennt normalerweise, dass sie Teilnehmer einer Konferenz ist, da in der Regel alle drei Beteiligte im Moment des Zusammenschaltens der Konferenz einen deutlich wahrnehmbaren Hinweiston zu hören bekommen. Dennoch besteht ein gewisses Risiko dafür, dass die angerufene Person meint, nur mit dem Anrufer zu sprechen und nicht erkennt, dass der ursprüngliche Gesprächspartner des Anrufers zuhört[6]. Dieses Risiko ist jedoch nicht höher einzustufen als das Risiko, durch Dritte mithilfe einer Freisprecheinrichtung am Telefon des Gesprächspartners abgehört zu werden.

G.28 Unerwünschtes Mithören

Anders als bei einer konventionellen Konferenz, in der sich sämtliche Teilnehmer im selben Raum befinden, kann es bei einer Telefonkonferenz durchaus unbemerkte Mithörer geben.

Schutzmaßnahmen siehe M.32, M.33, M.34

6.2.2 Push-to-Talk

Bei Push-to-Talk gibt es aus technischer Sicht aktuell keine dienstspezifischen zusätzlichen Gefährdungen, die man bei Nutzung der zu Grunde liegenden Übertragungsdienste nicht auch hätte. Gefährdungen können sich dennoch aus Fehlbedienung und fehlender Verschlüsselung ergeben.

G.29 Fehlbedienung

Mittels Push-to-Talk können nicht nur einzelne Empfänger angesprochen werden, sondern es können Empfängergruppen definiert werden, deren Mitglieder die jeweiligen Nachrichten empfangen. Fehler bei der Einrichtung der Empfängergruppen können dazu führen, dass Nachrichten an unerwünschte Empfänger geleitet werden.

Schutzmaßnahmen siehe M.35

G.30 Fehlende Verschlüsselung und Authentifizierung

Es ist zu vermuten, dass die Übertragung von Sprachdaten nach dem Standard PTT over Cellular (PoC) unverschlüsselt stattfindet. Auch eine Authentifizierung der Teilnehmer findet nicht statt.

Schutzmaßnahmen siehe M.1, M.2

[6] Im Festnetz konnte dieses Szenario unter Verwendung von ISDN-Telefonapparaten, die über zwei Sprachkanäle verfügen, erfolgreich gezeigt werden. Hier kann die Vermittlungsstelle keine Hinweistöne einspielen, da sie von einer Konferenz nichts weiß; aus Sicht der Vermittlungsstelle werden zwei unabhängige Gespräche geführt.

6.2.3 Mehrwertdienste

G.31 Benutzung von Mehrwertdiensten durch Unachtsamkeit

Durch unerwünschte E-Mail (Spam), Kurznachrichten oder „One Ring Calls“, die als unbeantwortete Anrufe angezeigt werden, können Nutzer dazu verleitet werden unbedacht Mehrwertdienste zu nutzen. So können z. B. hohe Kosten durch einen Rückruf zu kostenpflichtigen Nummern entstehen.

Schutzmaßnahmen siehe M.27, M.28, M.30, M.31

G.32 Verschleierung von Mehrwertdiensten

Zuweilen werden z. B. in Anzeigen verschleiert dargestellte Mehrwertrufnummern angegeben, welche beim Anrufen z.T. hohe Kosten verursachen. So fällt es in der Schreibweise „00 49 13 75 12 22 56“ nicht sofort auf, dass es sich um eine 0137er-MABEZ-Rufnummer handelt.

Schutzmaßnahmen siehe M.29, M.30

6.3 Mögliche Schutzmaßnahmen

Die folgenden Schutzmaßnahmen beziehen sich als Gesamtheit auf die Gefährdungen bei Nutzung der oben genannten Telefondienste. Da die Maßnahmen teilweise auf mehrere der aufgeführten Dienste anzuwenden sind, wurde keine Untergliederung der Maßnahmen nach Diensten vorgenommen.

M.27 Sperrung von unerwünschten Mehrwertdiensten

Nicht erwünschte Mehrwertdienste sollten gezielt beim Mobilfunkbetreiber gesperrt werden.

M.28 Achtsamkeit bei Rückrufen

Rückrufe auf versäumte Anrufe unbekannter Rufnummern sollten vermieden werden, insbesondere dann, wenn es sich um Rufnummern von Mehrwertdiensten handelt.

M.29 Achtsamkeit bei unbekannten Rufnummern

Alle unbekannten Rufnummern sollten vor dem Wählen aufmerksam verifiziert werden, um z. B. den Anruf von verschleiert angegebenen Mehrwertrufnummern wie z. B. „00 49 13 75 12 22 56“ zu vermeiden.

M.30 Sofortiges Beenden des Gesprächs

Bei Verdacht auf eine versehentliche Verbindung zu einer beliebigen Mehrwertrufnummer sollte spätestens innerhalb von 3 Sekunden nach der Ansage der Preisinformation die Verbindung getrennt werden, da sonst ein Vertragsverhältnis zustande kommt.

M.31 Informationen weiterleiten

Die Bundesnetzagentur sollte über Rufnummern- oder SMS-Spam informiert und gegebenenfalls Anzeige erstattet werden.

M.32 Vermeiden von automatischen Anrufannahmen

Eine automatische Rufannahme soll nur dann konfiguriert werden, wenn sie tatsächlich benötigt wird (z. B. im Auto ohne Freisprecheinrichtung, bei Nutzung des Endgerätes mit Ohrhörer).

M.33 Erhöhte Achtsamkeit bei Verwendung von Mobiltelefonen

Mobiltelefone sollten mit Umsicht genutzt werden. Insbesondere sollten die Ursachen für Warntöne und andere ungewöhnliche Geräusche während des Gesprächs unmittelbar überprüft werden. Zudem muss bei sensiblen Gesprächsinhalten sorgfältig geprüft werden, ob sich unerwünschte Mithörer in Hörweite befinden. Durch Antworten des lokalen Teilnehmers könnten Rückschlüsse auf den Inhalt des Gesprächs gezogen werden.

M.34 Sensibilität bei Benutzung von Freisprecheinrichtungen

Freisprecheinrichtungen sollten mit der notwendigen Sorgfalt genutzt werden. Wie auch bei Telefonaten ohne Freisprecheinrichtung muss sicher gestellt sein, dass keine unerwünschten Mithörer das Gespräch verfolgen können. Die Gefährdung wird bei Verwendung von Freisprecheinrichtung dadurch erhöht, dass der gesamte Wortlaut des Dialogs mitgehört werden kann.

M.35 Übersichtlichkeit erhalten

Empfängergruppen sollten übersichtlich benannt, sortiert und gepflegt werden. Dies hilft dem Benutzer, bei Verwendung von PTT und ähnlichen Diensten, berechtigte und unberechtigte Empfängergruppen zu unterscheiden.

7. Kurzmitteilungs-Dienst

7.1 Technische Grundlagen

Der seit Dezember 1992 verfügbare Kurzmitteilungsdienst (Short Message Service, SMS) bietet die Möglichkeit, kurze Nachrichten über das GSM zu übertragen. Der Dienst nutzt den Signalisierungskanal, der normalerweise für den Rufaufbau verwendet wird, zur Übertragung der Nachrichten[7]. Demzufolge kann die Übertragung einer Kurznachricht parallel zu einem laufenden Gespräch erfolgen.

Kurznachrichten – häufig auch als SMS bezeichnet – lassen sich nicht nur zwischen Mobiltelefonen austauschen, sondern auch mit anderen Systemen, insbesondere mit Servern von Dienstanbietern. So kann ein Anwender mittels Kurznachricht Aktionen beim Dienstanbieter auslösen, z. B. Anfordern einer Datei (z. B. „Klingelton“), die ihrerseits in einer Kurznachricht transportiert wird.

Darüber hinaus kann ein Netzbetreiber Kurznachrichten an alle in einer bestimmten Mobilfunkzelle angemeldeten Geräte versenden; diese Form der Kurznachricht nennt man Cell Broadcasts. Der Cell Broadcast ist mit einer Nummer markiert, die vom Endgerät akzeptiert werden muss. Bei den maximal 93 Zeichen langen Cell Broadcasts handelt es sich im Allgemeinen um Informationsdienste; einige Mobilfunk-Anbieter steuern über Cell Broadcasts die Darstellung bestimmter Tarifzonen am Endgerät[8], in denen sich der Anwender befindet.

Die Größe einer Kurznachricht ist auf 1120 Bit begrenzt. Um diesen Speicherplatz universell nutzen zu können bestehen drei verschiedene SMS-Codierungen:

- 7 Bit pro Zeichen für die Darstellung und Übertragung von Textnachrichten. Es können sowohl lateinische als auch große griechische Buchstaben dargestellt werden. Ausnahmen stellen hier jedoch Sondersymbole wie das €-Zeichen dar, die mit zwei 7 Bit Einheiten übertragen werden. 1120 Bit / 7 Bit = 160 Zeichen maximal.
- 8 Bit pro Zeichen bei Übertragung von binären Inhalten wie Logos, Klingeltönen oder Bildmitteilungen. 1120 Bit / 8 Bit = 140 Zeichen maximal.
- 16 Bit pro Zeichen zur Übertragung alternativer Zeichensätze, z. B. bei Nachrichten auf Arabisch, Hebräisch und Kyrillisch. 1120 Bit / 16 Bit = 70 Zeichen maximal.

Eine Kurznachricht bietet außerdem die Möglichkeit, die Verarbeitung auf dem Endgerät bereits beim Versenden der Nachricht festzulegen. So lassen sich z. B. sogenannte Flash-SMS versenden. Diese Kurznachrichten werden auf dem Endgerät ohne weiteres Zutun des Benutzers sofort angezeigt und meist nicht im SMS Speicher abgelegt. Auf diese Weise werden z. B. Werbenachrichten des Netzbetreibers oder Willkommens Kurznachrichten von Roaming

---

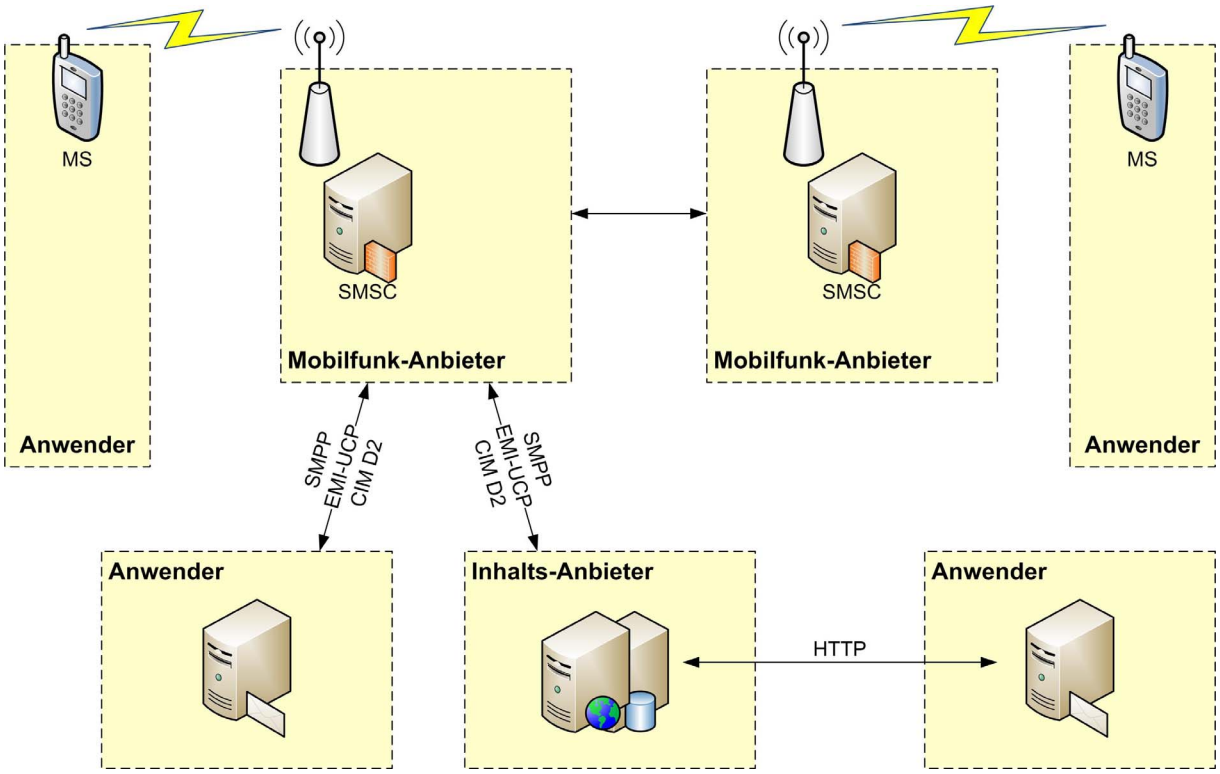
[7] Diese Idee wurde bereits früher bei ISDN verwirklicht, indem man Paket-Daten über den zur Signalisierung verwendeten D-Kanal übertragen hat (X.31)

[8] Typischer Anwendungsfall ist die sogenannte Homezone, aus der sich mit besonders günstigen Tarifen telefonieren lässt.

Partnern versendet. Eine weitere spezielle Versandart ist das Versenden einer Silent Message. Diese Kurznachricht wird einmalig vom Endgerät verarbeitet, jedoch weder angezeigt, gespeichert noch akustisch gemeldet. Über diese Versandart der SMS werden z. B. Ortungen von Mobiltelefonen durchgeführt oder vom Netzbetreiber Konfigurationen am Endgerät vorgenommen.

Da der Versand von Kurznachrichten ausschließlich auf den im GSM bereits vorhandenen Mechanismen basiert, unterliegen sie der gleichen Verschlüsselung, die auch Sprache und Signalisierung zuteil wird (siehe Kapitel 1.1.3). Hierbei handelt es sich aber nicht um eine Ende-zu-Ende-Verschlüsselung, das heißt die Kurznachrichten liegen zwischenzeitlich unverschlüsselt innerhalb des Mobilfunknetzes vor. Abhilfe kann hier Kryptosoftware schaffen, die den Inhalt von Nachrichten vor der Übertragung nach einem beliebig starken Verfahren verschlüsselt. Auf der Seite des Empfängers wird dann mit demselben Verfahren entschlüsselt. So ist der Inhalt der Nachricht auf dem kompletten Übertragungsweg gesichert. Dies gilt aber nur für den Inhalt, nicht für die enthaltenen Routinginformationen.

Abbildung 14: Architektur zur Übertragung von Kurzmitteilungen (vereinfacht)



Kern der Kurzmitteilungsdienste ist das Short Message Service Center (SMSC). Es ist auf der einen Seite in das Mobilfunknetz eingebunden, um SMS-MT (SMS Mobile Terminated) an Endgeräte ausliefern zu können bzw. SMS-MO (SMS Mobile Originated) von diesen entgegennehmen zu können. Außerdem bestehen Verbindungen zu anderen Mobilfunk-Anbietern, damit Kurzmitteilungen auch mit Teilnehmern anderer Mobilfunknetze ausgetauscht werden können.

Für den massenweisen Versand und Empfang von SMS im Geschäftsumfeld („Large Account“) stellen die Mobilfunkprovider ihren Kunden direkte Zugänge auf das SMSC zur Verfügung. Dies kann direkt, z. B. per Standleitung, oder über ein Gateway im Internet erfolgen. Es sind entsprechende Verträge mit dem Mobilfunk-Anbieter zu schließen, der den Zugriff

auf das SMSC erlaubt und die entsprechende Software bereitstellt[9]. Solche Dienste werden nicht nur von Mobilfunk-Anbietern direkt angeboten, sondern auch von Dritten im In- und Ausland. Sie sind damit prinzipiell für beliebige Personen verfügbar.

Die Einlieferung von Kurzmitteilungen an das SMSC kann mit einer Vielzahl von Protokollen erfolgen, unter anderem:

- SMPP (Short Message Peer to Peer), ein ursprünglich von Logica entwickeltes Protokoll, das später vom SMS-Forum – welches inzwischen aufgelöst wurde - weiterentwickelt wurde.
- EMI-UCP (External Machine Interface) geht auf das Universal Computer Protocol (UCP) zurück, das bei der ETSI unter ETS 300 133-3 (siehe [ETS300]) standardisiert ist. Es war ursprünglich zur Einlieferung von Nachrichten in das ERMES (European Radio Message System) gedacht. Es wurde um spezielle Aspekte der Kurzmitteilungen erweitert, insbesondere durch den Hersteller CMG.
- CIMD2 (Computer Interface to Message Distribution), ein vom Hersteller Nokia entwickeltes Protokoll
- TAP (Telecator Alphanumeric Protocol), ein vom Hersteller Motorola entwickeltes Protokoll

Am Markt sind verschiedene Computer-Programme verfügbar, die Kurzmitteilungen über derartige Protokolle an ein SMSC einliefern können. Darüber hinaus wird auch die Einlieferung von SMS über Browser mittels HTTP (Hypertext Transfer Protocol) angeboten. Da durch den Versand von SMS Kosten entstehen, erfordern die Mobilfunkbetreiber eine Authentisierung des Einlieferers einer SMS.

7.1.1 EMS

Der Enhanced Message Service beruht auf der Aneinanderreihung von mehreren SMS-Kurznachrichten, die vom Netzbetreiber als einzelne SMS-Kurznachricht abgerechnet werden. Der so gewonnene Speicherplatz für die Übertragung von n x 160 Zeichen bietet genug Raum, um kleinere Logos, Bilder oder sogar Klingeltöne zu übertragen. Technisch besteht z. B. eine 541 Zeichen lange EMS-Nachricht aus vier SMS-Kurznachrichten.

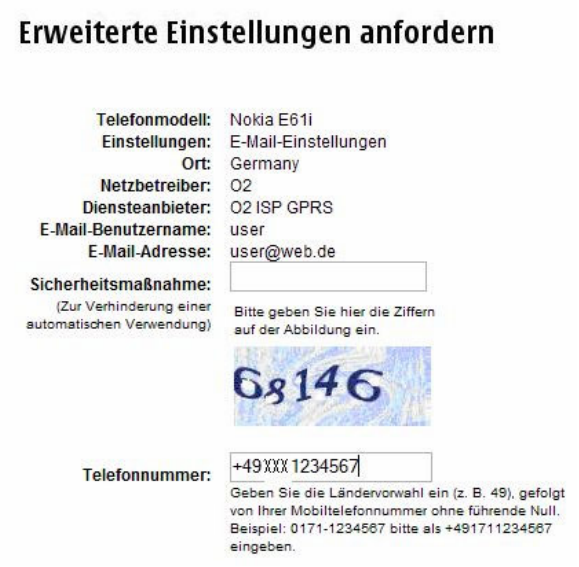
7.1.2 „Over the Air“-Konfiguration (OTA Provisioning)

Mithilfe spezieller Kurznachrichten lassen sich Konfigurationseinstellungen an mobile Endgeräte übermitteln. Das Verfahren wird häufig als Over the Air (OTA) Provisioning bezeichnet. OTA Provisioning erlaubt einem Mobilfunk-Anbieter, die für sein Netz spezifischen Einstellungen für die GPRS-Verbindungskonfiguration, für MMS (siehe Kapitel 9) oder für die Synchronisation von E-Mail, Kalender-Einträgen und Kontakten an den Anwender zu übertragen. Dadurch wird dem Anwender die Konfiguration seines Endgerätes erheblich erleichtert. Abbildung 15 zeigt als Beispiel das Anfordern von Einstellungen für ein E-Mail-Konto.

[9] Etwa als „Plugin“ für gängige Groupware- oder Mail-Lösungen

OTA Provisioning erlaubt darüber hinaus auch die Übertragung von Gerätesoftware („Firmware“) an ein mobiles Endgerät. Diese Variante wird mit „Firmware over the air“ (FOTA) bezeichnet.

Abbildung 15: Anfordern von Geräteeinstellungen (Quelle: Nokia)



Die Konfigurationseinstellungen werden bei den meisten Endgeräten einem Standard der Open Mobile Alliance (OMA) entsprechend übertragen (siehe [OMAcont]). Der Standard formatiert die Befehle als XML-Tags (Extensible Markup Language) und entsprechende Attribute. Die binäre Codierung des XML erfolgt anhand der „Binary XML Content Format Specification“ des WAP-Forums (siehe [WAP192]), die auch Basis für WAP ist (siehe Kapitel 8). Konfigurationseinstellungen bestehen im Allgemeinen aus mehreren aneinandergereihten Kurznachrichten.

Gegen den Empfang von OTA Provisioning SMS gibt es keine Schutzmaßnahmen für den Nutzer. Das Löschen des SMSC-Eintrags im eigenen Mobiltelefon führt nur dazu, dass keine Kurzmitteilungen mehr versendet werden können – der Empfang funktioniert jedoch nach wie vor.

7.2 Sicherheitsgefährdungen für den Nutzer

Aus den Diensten SMS und EMS sowie der providerseitigen Nutzung von OTA ergibt sich eine Reihe von Sicherheitsgefährdungen.

G.33 Kurznachrichteninhalte sind nicht geschützt

Kurznachrichten werden im Short Message Service Center (SMSC) unverschlüsselt gespeichert.

Schutzmaßnahmen siehe M.36

G.34 Denial-of-Service-Angriff per SMS

Hierbei wird eine große Zahl SMS-Kurznachrichten in kurzer Zeit an das Mobiltelefon versendet („SMS-Bombe“), das dadurch nur noch eingeschränkt zu gebrauchen

ist. Darüber hinaus konnten in der Vergangenheit Softwarefehler in bestimmten Mobiltelefonen dazu ausgenutzt werden, um per SMS-Kurzmitteilung einen Buffer Overflow zu erzeugen, der einen Absturz des Mobiltelefons zur Folge hat (siehe [PrPo50781]).

Schutzmaßnahmen siehe M.37, M.39

G.35 Silent Messages

Diese werden auf dem Mobiltelefon weder angezeigt noch gespeichert. Sie können zur Vorbereitung einer Ortung verwendet werden.

Schutzmaßnahmen siehe M.4

G.36 Over-the-air-Konfiguration

Verändern der Konfiguration eines Mobiltelefons per „Over the air“ (OTA) Provisioning.

Schutzmaßnahmen siehe M.38

G.37 Spam-SMS

Mit Spam-SMS soll der Empfänger motiviert werden, eine nicht klar erkennbare teure Rückrufnummer zu wählen.

Schutzmaßnahmen siehe M.27, M.28, M.29, M.39

G.38 SMS mit gefälschtem Absender

Bestimmte Anbieter im Internet lassen die Versendung von SMS-Kurznachrichten zu, bei denen als Absender Freitext eingegeben werden darf. Dies kann neben der Kenntnisnahme von gefälschten Informationen insbesondere in Kombination mit OTA Provisioning (siehe G.36) zu unerwünschten Konfigurationsänderungen bis hin zu einem kompletten Austausch der Geräte-Firmware führen.

Kein Schutz gegen den Erhalt möglich, ansonsten siehe M.38

G.39 Abhören gesendeter Daten

Wird durch ein öffentliches Netz, etwa per TCP/IP über das Internet, auf ein SMSC oder Gateway des Dienstleisters zugegriffen, besteht für diese Übertragungswege die Gefahr der Manipulation oder des Abhörens der übertragenen Daten.

Schutzmaßnahmen siehe M.40, M.41

G.40 Innentäterproblematik

Ein Innentäter mit direktem Zugriff auf das Netz des Mobilfunk-Anbieters oder Dienstleisters kann die gesendeten Daten an den Schnittstellen zum SMSC manipulieren oder abhören. Auch die Rekonstruktion von Geschäftsbeziehungen des Kunden ist denkbar.

Schutzmaßnahmen siehe M.41

G.41 Identitätsdiebstahl

Durch den Missbrauch von Kundenaccounts können zum Beispiel Massen-SMS auf Kosten des Kunden versandt werden (Spam) oder Denial-of-Service-Angriffe auf beliebige Mobiltelefonnummern ausgeführt werden.

Schutzmaßnahmen siehe M.42

7.3 Mögliche Schutzmaßnahmen

Durch die folgenden Sicherheitsmaßnahmen können sowohl die Gefährdung durch SMS/EMS als auch durch OTA Provisioning minimiert werden.

M.36 SMS-Verschlüsselung

Wenn vertrauliche Informationen per SMS zu übertragen sind, muss eine Verschlüsselung der SMS-Kurznachrichten durch die Mobiltelefone erfolgen. Hierzu ist entsprechende Software auf den Mobiltelefonen der Kommunikationspartner zu installieren.

M.37 Schließen von Sicherheitslücken

Firmware Update des Mobiltelefons, um bekannt gewordene Fehler zu beseitigen

M.38 Gesunder Menschenverstand

Jede Kurzmitteilung sollte objektiv auf den Wahrheitsgehalt von Absender und Inhalt geprüft werden. Im Zweifelsfall sollte ein bekannter Absender für Rückfragen kontaktiert werden; dabei sind keinesfalls die im Nachrichtentext genannten unbekannten Rückrufnummern zu verwenden! Bei unbekanntem Absender und zweifelhaftem Inhalt sollte die Nachricht gelöscht werden. Die Verarbeitung von OTA Provisioning SMS, d. h. der Konfigurationseinstellungen, sollte generell abgelehnt werden, wenn diese nicht nach vorangegangener expliziter Absprache angekündigt wurde, z. B. durch einen Anruf im Service Center des Mobilfunkbetreibers mit der Frage nach den korrekten GPRS-Einwahldaten.

M.39 Anrufsperre für SMS

Der Empfang von SMS-Kurznachrichten lässt sich bereits beim Mobilfunk-Anbieter vollständig sperren. Das Aktivieren bzw. Deaktivieren der Sperre erfolgt durch den Anwender über spezielle Codes, die an der Tastatur des Mobiltelefons eingegeben werden. Voraussetzung ist jedoch im Allgemeinen eine vorhergehende Freischaltung der Sperr-Möglichkeit durch den Mobilfunk-Anbieter. Alternativ lassen sich am Mobiltelefon eingegangene SMS nach bestimmten Kriterien filtern. Hierzu ist in der Regel zusätzliche Software auf dem Mobiltelefon zu installieren.

M.40 Datenverschlüsselung

Falls keine angemieteten dedizierten Leitungen von einem Kunden zum SMSC bzw. Gateway eines Mobilfunk-Anbieters verwendet werden, ist eine Verschlüsselung der Datenübertragung zwingend notwendig. Falls diese nicht bereits durch den Anbieter vorgesehen ist, muss eine dienstunabhängige Lösung zwischen Anbieter und Kunde, z. B. mittels VPN-Tunnel, implementiert werden.

M.41 Implementierung von Sicherheitskonzepten

Falls ein externer Dienstleister den Zugang zum SMSC des Mobilfunk-Anbieters zur Verfügung stellt, muss ein durchgängiges Sicherheitskonzept von SMSC bis zum Kunden durch den Dienstleister nachgewiesen werden.

M.42 Übertragungsvolumen festlegen

Um den möglichen Missbrauch eines SMS-Accounts für Massen-SMS und „SMS-Bomben“ einzuschränken, sollte ein fixes Übertragungsvolumen mit dem Provider vereinbart werden. Dieses sollte die reellen Bedürfnissen innerhalb eines Zeitraums widerspiegeln und nach Bedarf erweitert werden können. So lassen sich eventuell durch einen Missbrauch entstehende Kosten eindämmen. Außerdem erleichtert dies die Erkennung eines ungewöhnlich hohen Nachrichtenaufkommens.

8. WAP und Internet-Dienste

Das Wireless Application Protocol (WAP) bietet die Möglichkeit, Internet-Seiten mithilfe von Mobiltelefonen darzustellen. Es gleicht in dieser Hinsicht dem Zugriff auf Internet-Seiten mittels HTTP. Darüber hinaus bietet WAP jedoch zwei zusätzliche Funktionalitäten:

- Unaufgeforderter Empfang von Inhalten über einen sogenannten Push-Dienst (WAP Push)
- Steuerung von Funktionen des Telefons durch die empfangenen Inhalte (Wireless Telephony Application, WTA)

Motivation für die Einführung von WAP waren – neben den oben genannten zusätzlichen Funktionalitäten – die besonderen Bedingungen bei der Anzeige von Inhalten des Internets auf Mobiltelefonen, insbesondere die eingeschränkte Bildschirmgröße und die geringe Bandbreite der Datenverbindung. Diese Bedingungen führten zu folgender Entwicklung:

- Eine eigene Beschreibungssprache für Inhalte (Wireless Markup Language, WML, siehe [WAP238]), die Text-basierte Befehle („Tags“) verwendet, die den Regeln von XML entsprechen. Es wird darüber hinaus eine aus ECMAScript[10] (siehe [ECMA262]) abgeleitete Sprache zur Beschreibung aktiver Inhalte bereitgestellt, die als WMLScript bezeichnet wird (siehe [WAP192]).
- Eine Codierung der Sprachelemente von WML und WMLScript in binärer Form zur effizienten Übertragung auf der Luftschnittstelle. Die Tags werden dabei in eine nur wenige Byte umfassende Form umgewandelt.
- Ein eigener Protokoll-Stack, der für die Übertragung auf Mobilfunkverbindungen mit niedriger Datenrate und mit einer gewissen Fehlerwahrscheinlichkeit optimiert ist (siehe [OMAWWP], [WAP210]).

8.1 Technische Grundlagen

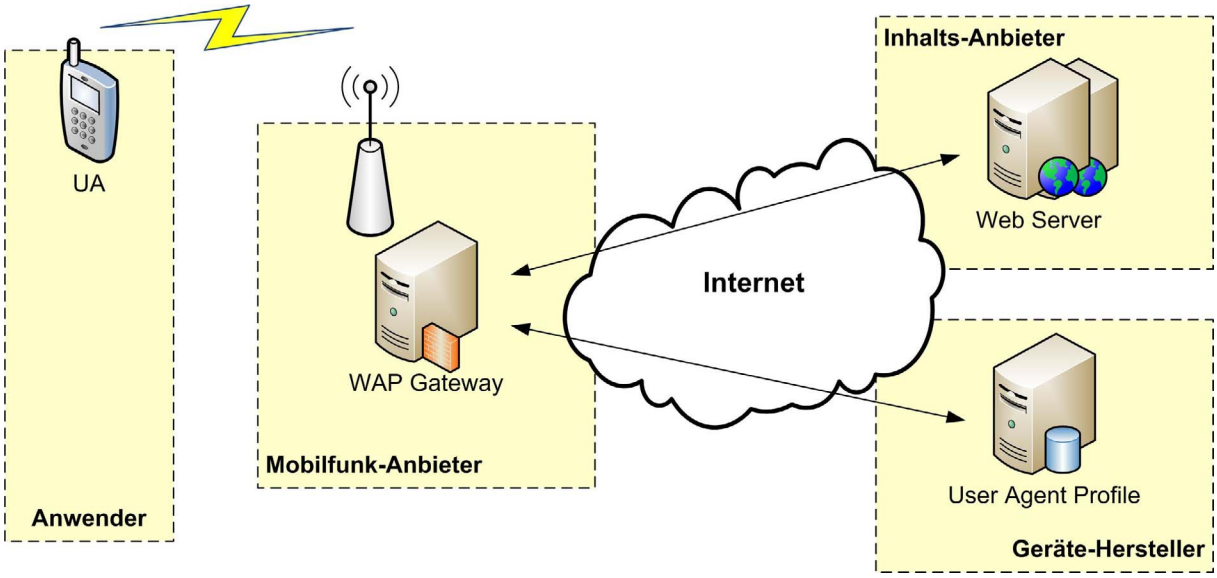
8.1.1 Architektur und Übertragungstechniken von WAP

Ein Anbieter im Internet stellt seine Inhalte auf Webservern in WML bereit. Der Mobilfunkprovider betreibt einen sogenannten WAP Gateway, der die Umwandlung der WML in die binäre Form vornimmt. Der WAP Gateway formatiert dabei die Inhalte derart, dass sie von dem Mobiltelefon (hier: User Agent, UA) bestmöglich dargestellt werden können. Das Mobiltelefon übermittelt dem WAP Gateway zu diesem Zweck ein entsprechendes User Agent Profile (UAProf)[11].

[10] Hinter ECMAScript verbirgt sich die standardisierte Version der bei HTML Browsern verwendeten Sprache JavaScript.

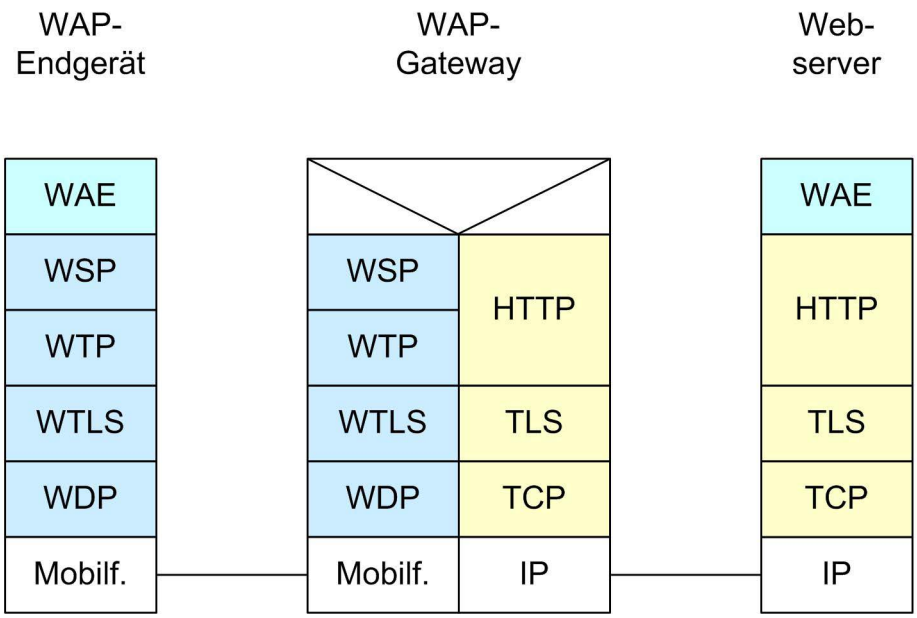
[11] Genau genommen übermittelt das Mobiltelefon dem WAP-Proxy nur ein URI, das auf das beim Gerätehersteller abzurufende UAProf weist, z. B. http://www.htcmms.com.tw/tmo/mdapro-1.3.xml

Abbildung 16: Architektur von WAP



Die in den Jahren bis 1999 vorgestellten WAP-Versionen 1.0 bis 1.2 wurden auf der Luftschnittstelle ausschließlich spezielle Protokolle vorgesehen, insbesondere das Wireless Session Protocol (WSP, siehe [WAP230]) und die Binary XML Content Format Specification (siehe [WAP192]), anhand derer die beschriebene Codierung der HTTP-Header und WML Tags in die binäre Form vorgenommen wird, das Wireless Transaction Protocol (WTP, siehe [WAP224] und das Wireless Datagram Protocol (WDP, siehe [WAP259]). Den vollständigen Protokoll-Stack von WAP 1.x, der die Netzzugangs-Ebene nicht spezifiziert, zeigt Abbildung 17. Der Begriff WAE steht dabei für das Wireless Application Environment (siehe [WAP236]), das die Fähigkeiten des User Agent und die unterstützten Datenformate beschreibt.

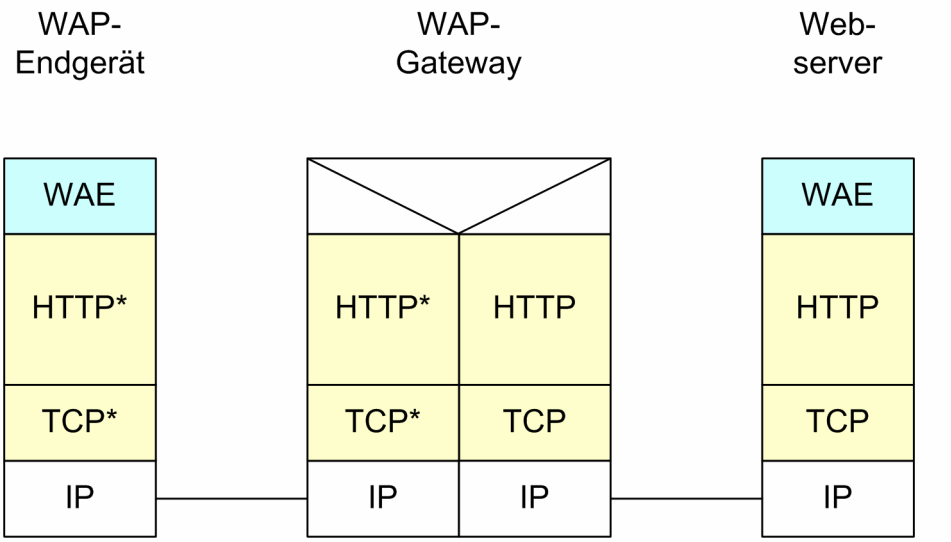
Abbildung 17: Protokoll-Stack von WAP 1.x (aus [WAP210])



In 2001 wurde die heute aktuelle WAP-Version 2.0 vorgestellt. Sie trägt dem gestiegenen Leistungsumfang von Mobilfunknetzen und Endgeräten Rechnung, indem sie den Zugriff auf

beliebige Seiten im Internet erlaubt. Hierfür wird nun auch auf der Luftschnittstelle die Protokoll-Ebenen HTTP, TCP und IP, aufsetzend auf der Netzzugangs-Ebene, genutzt. Zusätzlich ändert sich mit WAP-Version 2.0 die Beschreibung der Inhalte. Diese erfolgt nun mit einer Variante der Markup-Sprache XHTML (Extensible Hypertext Markup Language), die von HTML (Hypertext Markup Language) abgeleitet ist und die Elemente der ursprünglichen WML enthält. Der Protokoll-Stack von WAP 2.0 ist in Abbildung 18 dargestellt.

Abbildung 18: Protokoll-Stack von WAP 2.0 (aus [WAP210])



Die Verwendung des WAP Gateway ermöglicht die Optimierung von TCP und HTTP auf spezielle Belange des Mobilfunks (HTTP*, TCP*), wie z. B. auf eine höhere Wahrscheinlichkeit von Paketverlusten. In WAP 2.0 ist auch der direkte Zugriff auf einen Webserver ohne zwischengeschaltetes WAP Gateway (Proxy) möglich. Allerdings kann in diesem Fall keine Protokoll-Optimierung erfolgen.

Mobiltelefone, die WAP 2.0 unterstützen, erlauben es häufig, bei der Einstellung des WAP Gateway eine Port-Nummer anzugeben. WAP Gateways für WAP 2.0 werden in der Regel über Port 8080 erreicht, Gateways für WAP 1.x über den Port 9201.

Für den Anwender ist in der Regel nicht klar zu erkennen, ob das Endgerät für einen Seitenaufruf WAP 1.x oder WAP 2.0 verwendet. Dies ist zum Teil noch nicht einmal aus den Datenblättern der Mobiltelefone ersichtlich, da dort häufig nicht zwischen den Markup-Sprachen und den Protokoll-Stacks unterschieden wird. Einige Mobiltelefone unterstützen nur den Protokoll-Stack von WAP 1.x, der Browser ist aber dennoch in der Lage XHTML-Seiten darzustellen. Die Datenblätter solcher Endgeräte weisen in der Regel die Unterstützung für WAP 1.x und WAP 2.0 aus. Neue Endgeräte unterstützen häufig nur noch den Protokoll-Stack WAP 2.0, dennoch können die Browser dieser Endgeräte WML-Seiten darstellen.

Ein sicheres Indiz für die Unterstützung und Verwendung des WAP-2.0-Protokoll-Stacks ist die Möglichkeit, auf Seiten im Internet direkt, d. h. unter Umgehung jeglicher Gateways und Proxys, zuzugreifen.

8.1.2 Übertragung bei WAP

Auf dem „Wireless Application Protocol“ basierende Internet-Dienste nutzen verschiedene Übertragungstechniken. Einerseits werden dafür alle Dienste eingesetzt, die dem Mobiltelefon eine direkte IP-Verbindung eröffnen, also unter anderem CSD, GPRS oder HSDPA. Andererseits ist eine Übertragung bestimmter Daten über GSM-spezifische Dienste wie SMS und USSD (Unstructured Supplementary Service Data) vorgesehen.

In WAP 1.x wurde als einheitliches Übertragungsprotokoll der OSI-Schicht 4 das Wireless Datagram Protocol (WDP) eingeführt (siehe [WAP259]). Der Standard beschreibt, wie WDP einerseits auf UDP und andererseits auf die für GSM und andere Mobilfunkdienste (z. B. auf TETRA (Terrestrial Trunked Radio) oder gar DECT) abgebildet wird. Mobiltelefone mit WAP 1.x nutzen in den Europäischen Mobilfunknetzen normalerweise UDP/IP als Basis für die Übertragung. Lediglich für den Spezialfall des WAP-Push (siehe Kapitel 8.1.3) wird ein GSM-spezifischer Dienst verwendet.

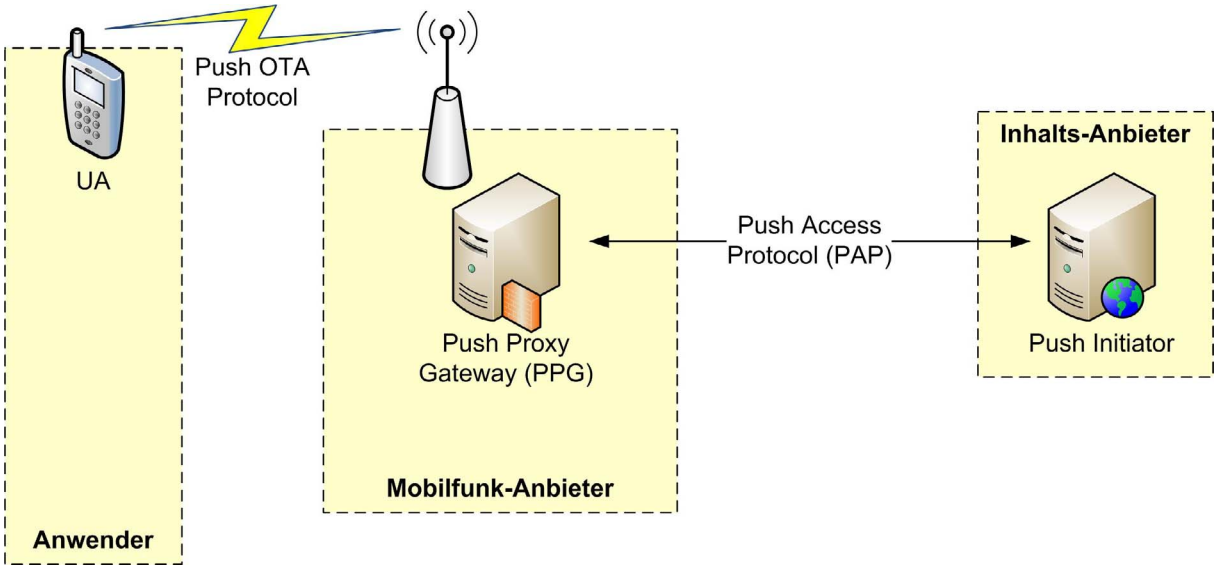
WAP 2.0 setzt unmittelbar auf HTTP und TCP/IP auf (siehe Abbildung 18). WDP wird nur noch für das WAP-Push benötigt.

8.1.3 WAP Push

Die Arbeitsweise des Anwenders beim Zugriff auf Internet-Seiten ist zunächst unabhängig davon, ob ein Mobiltelefon mit WAP oder ein Personalcomputer mit HTML genutzt wird. Der Zugriff erfolgt grundsätzlich vom Anwender getrieben; es handelt sich um eine „Pull-Technik“. WAP stellt darüber hinaus mit „WAP Push“ eine Technik bereit, die es einem Server ermöglicht, ohne Zutun des Anwenders Internet-Seiten auf dem Mobiltelefon darzustellen oder andere Aktionen auszuführen. WAP Push bietet insbesondere die Möglichkeit, auch andere Anwendungen des Mobiltelefons anzusteuern als den WAP Browser. Der wichtigste Anwendungsfall für WAP Push ist das Ausliefern von Multimedia-Mitteilungen (siehe Kapitel 9).

Bei WAP Push übermittelt der Server des Inhalts-Anbieters – hier Push Initiator genannt – eine Nachricht zu einem Gateway beim Mobilfunk-Anbieter. Der Gateway wird als Push Proxy Gateway (PPG) bezeichnet; das entsprechende Protokoll heißt Push Access Protocol (PAP).

Abbildung 19: Architektur von WAP Push



Das PAP verwendet ein Nachrichtenformat, das auf HTTP basiert. Im HTTP Header befinden sich einige WAP-spezifische Angaben z. B. bezüglich der Applikation auf dem Mobiltelefon, mit der die Push-Nachricht bearbeitet werden soll. Auf den HTTP-Header folgt im Allgemeinen eine Nachricht, die aus mehreren Teilen besteht (Multipart Message).

1. Erster Teil dieser Nachricht ist das in XML codierte PAP, das Informationen für die weitere Verarbeitung durch den PPG enthält. Dies sind insbesondere der Nachrichtenempfänger (d. h. Telefonnummer) und der auf der Luftschnittstelle zu verwendende Transportdienst. Als Transportdienst kann sowohl eine bestehende Verbindung über HTTP als auch ein GSM-spezifischer Dienst verwendet werden.

Abbildung 20: Beispiel für den PAP-Teil eines WAP-Push

```
<pap>
  <push-message
    push-id="230_1078839209473_1038@mr-00.              .de"
    deliver-before-timestamp="2004-03-10T01:33:23Z">
    <address
      address-value="WAPPUSH=+4917      63/TYPE=PLMN@10.2.172.140">
      </address>
    <quality-of-service
      priority="medium"
      delivery-method="unconfirmed"
      bearer="SMS"
      bearer-required="true">
      </quality-of-service>
    </push-message>
  </pap>
```

2. Der zweite Teil der Nachricht enthält den eigentlichen Inhalt. Er wird entweder als sogenannte Service Indication (SI) oder als Service Load (SL) typisiert. Beide Inhalts-Typen besitzen einen Verweis (Uniform Resource Identifier, URI) auf den vom WAP Browser des Mobiltelefons über eine TCP/IP-Verbindung zu ladenden Inhalt. SI präsentiert dem Anwender zuvor einen Hinweis auf die Nachricht; der Inhalt wird erst ge-

laden, wenn der Anwender dies explizit bestätigt. SL lädt den Inhalt unmittelbar nach Erhalt der Nachricht.

Da der Versender eines WAP-Push im Allgemeinen nicht davon ausgehen kann, dass das Mobiltelefon über eine aktivierte Internetverbindung verfügt, wird er einen Kommunikationskanal wählen, der immer zur Verfügung steht. Diese Rolle kommt dem Kurznachrichtendienst (SMS) zu. Alle Mobiltelefone im europäischen Raum unterstützen heute SMS und die entsprechende Infrastruktur (SMSC) ist bei allen Mobilfunk-Anbietern vorhanden. Es ist daher davon auszugehen, dass WAP-Push im Allgemeinen auf Basis von SMS durchgeführt wird.

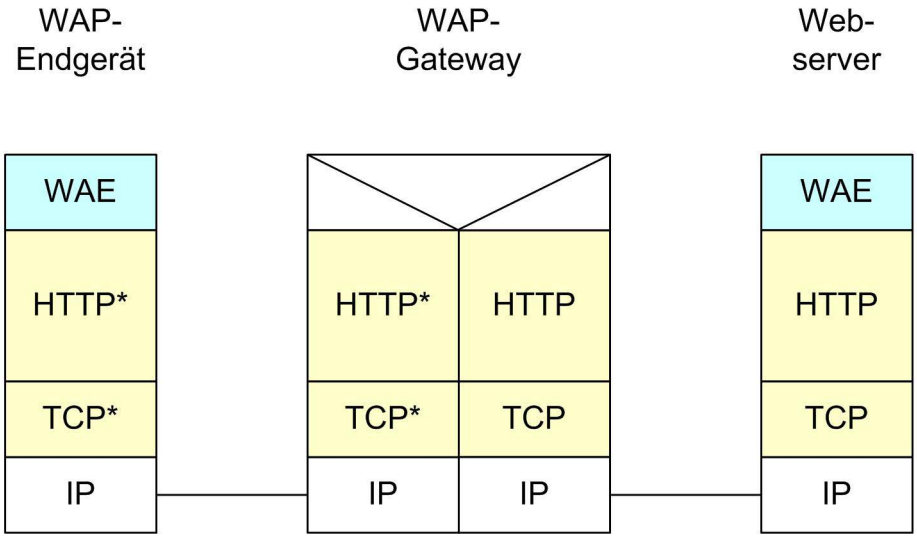
8.1.4 Verschlüsselung bei WAP

Vertraulichkeit und Integrität der Datenübertragung wird bei allen Varianten von WAP mittels Transport Layer Security (TLS) sichergestellt. Bei WAP 1.x kommt hierfür ein eigenes Protokoll (Wireless Transport Layer Security, WTLS, siehe [WAP261]) zum Einsatz, das auf TLS 1.0 (siehe [RFC2246]) basiert. WTLS ist – wie die übrigen Protokolle von WAP 1.x – auf geringe Datenraten und lange Laufzeiten optimiert. Darüber hinaus trifft WTLS Maßnahmen für einen verlässliche Durchführung der Protokollabläufe („Handshakes“), da es sich im Gegensatz zu TLS auf das verbindungslose Protokoll WDP stützt (siehe Abbildung 17).

WTLS unterstützt mehrere Block-Chiffren mit Cipher Block Chaining (CBC) auf Basis der Algorithmen RC5, IDEA und 3DES. Die maximalen Schlüssellängen betragen 128 Bit bei RC5 und IDEA bzw. 168 Bit bei 3DES. Es werden jedoch auch Schlüssel mit Längen von 40 und 56 Bit zugelassen.

Mittels WAP 2.0 kann ein Mobiltelefon auf beliebige Internet-Seiten mittels HTTP zugreifen. Dementsprechend wird Authentifizierung und Verschlüsselung per TLS unterstützt, sodass eine sichere Verbindung unmittelbar mit dem Server des Inhalts-Anbieters im Internet aufgebaut werden kann. Da im Allgemeinen ein WAP-Gateway eingesetzt wird, das die Funktion eines HTTP-Proxy übernimmt (siehe Abbildung 18), muss das Mobiltelefon die TLS-Verbindung mithilfe der Methode „CONNECT“ des HTTP aufbauen. Somit entsteht ein TLS-Tunnel gemäß [RFC2817], wie in folgender Abbildung dargestellt.

Abbildung 21: Verschlüsselter Tunnel zum Webserver bei WAP 2.0



Der Standard definiert drei Klassen der Implementierung, die sich in verschiedenen Punkten unterscheiden. Die folgende Tabelle gibt eine Übersicht der Klassen.

Tabelle 5: Klassen bei WTLS (O = Optional, E = Erforderlich)

Merkmal	Klasse 1	Klasse 2	Klasse 3
Austausch öffentlicher Schlüssel	E	E	E
Prüfung von Server-Zertifikaten	O	E	E
Prüfung von Client-Zertifikaten	O	O	E
Unterstützung voreingestellter geheimer Schlüsselpaare	O	O	O
Datenkompression	-	O	O
Verschlüsselung	E	E	E
Integritätsprüfung (Message Authentication Code, MAC)	E	E	E
Schnittstelle zu Smartcard	-	O	O

Die in Tabelle 5 genannte Schnittstelle zu Smartcards bezeichnet eine Erweiterung des Standards, die sich WAP Identity Module (WIM) nennt [WAP260]. WIM bietet einen sicheren Speicherort für Client-Zertifikate inklusive der geheimen Schlüssel. WIM könnte z. B. als Teil einer SIM-Karte in einem Mobiltelefon implementiert werden.

8.1.5 Wireless Telephony Application (WTA)

WTA (siehe [WAP266]) stellt eine Erweiterung des WAE um die Möglichkeit dar, Funktionen der Mobiltelefone mittels WAP-Nachrichten, d. h. mittels WML und WMLScript, steuern zu können. Das WTA erweitert das WAE unter anderem um Folgendes:

- Eine Schnittstelle von WML und WMLScript zu internen Funktionen des Mobiltelefons (Wireless Telephony Application Interface, WTAI, siehe [WAP268]). Über das WTAI lassen sich Telefonanrufe ausführen, Kurzmitteilungen versenden, das Telefonbuch mo-

difizieren sowie Anruflisten auslesen. Darüber hinaus ermöglicht das WTAI die Verarbeitung eingehender Anrufe und Nachrichten.

- Reaktionsmöglichkeit auf bestimmte Ereignisse im Mobilfunknetz
- Einen Speicherbereich zur dauerhaften Installation von WAP-Inhalten (WML, WMLScript, Bilder usw.), die ereignisgetrieben in „Echtzeit“ ausgeführt werden können
- Ein Sicherheitsmodell

Das Sicherheitsmodell von WTA sieht vor, dass jegliche Kommunikation mittels WTLS Klasse 2 (siehe [WAP261]) abzusichern ist. Das Mobiltelefon kommuniziert ausschließlich über ein WAP Gateway, dem es vertraut (Trusted Gateway). Der WAP Gateway authentisiert sich zu diesem Zweck am Mobiltelefon mit einem Server-Zertifikat, dessen Gültigkeit der Client überprüfen kann. Der Betreiber des Trusted Gateway – also normalerweise der Mobilfunk-Anbieter – muss sicherstellen, dass nur vertrauenswürdige Inhalts-Anbieter Funktionen des WTA nutzen können. Der Standard schreibt hierzu aber keine Sicherheitsmechanismen explizit vor.

8.2 Sicherheitsgefährdungen für den Nutzer

G.42 Keine Ende-zu-Ende-Verschlüsselung bei WAP 1.x

Die Vertraulichkeit einer verschlüsselten Verbindung bei WAP 1.x (WTLS) ist nicht gewährleistet. Der WAP-Gateway ist sowohl aus Sicht des Mobiltelefons als auch aus der Sicht der Anwendung im Internet der Endpunkt des verschlüsselten Kanals. Die Daten passieren das WAP Gateway somit unverschlüsselt. Dadurch ist es einem Angreifer prinzipiell möglich, geheime Informationen auszuspähen, wenn er Zugriff auf das WAP Gateway besitzt.

Schutzmaßnahmen siehe M.43

G.43 Ausführung aktiver Inhalte

Die Ausführung aktiver Inhalte, d. h. nicht sichtbarer Funktionen, die in Internet-Seiten mit ECMAScript bzw. WMLScript und empfangenen Push-Nachrichten verborgen sein können, birgt Sicherheitsrisiken wie beispielsweise die Verbreitung von „Handy-Viren“ und „Handy-Trojanern“. Der Nutzer kann nicht ohne Weiteres erkennen, welche Funktionen sich im Einzelnen in einer MMS verbergen, und hat keine Kontrolle darüber, in welcher Form auf das Endgerät zugegriffen wird und welche Änderungen möglicherweise vorgenommen werden.

Schutzmaßnahmen siehe M.44, M.45, M.46

G.44 Unbemerkter Internetverbindungsaufbau

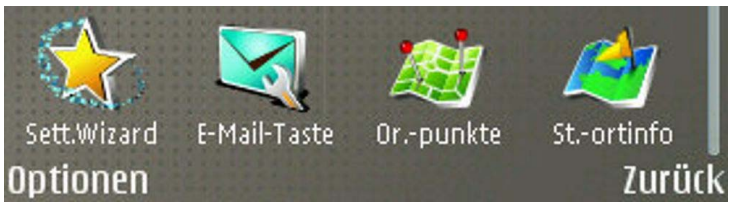
Ein unbemerkter Aufbau einer Datenverbindung durch Fehlbedienung und damit die ungewollte Exposition des Endgerätes zum Internet ist möglich. Insbesondere die von den Mobilfunk-Anbietern auf die Endgeräte aufgebrachten Standard-Konfigurationen („Brandings“) erschweren häufig eine fehlerlose Bedienung. Typischerweise belegen Mobilfunk-Anbieter diejenige Taste des Hauptmenüs mit dem Internetzugang (rechte Taste in Abbildung 22), die in Untermenüs zum Schließen

derselben verwendet wird (entsprechende Taste in Abbildung 23). Schließt der Anwender ein Untermenü und drückt dabei die „Zurück“-Taste einmal zu viel, wird er mit dem Internet verbunden.

Schutzmaßnahmen siehe M.47

Abbildung 22: Hauptmenü eines Mobiltelefons

Abbildung 23: Untermenü eines Mobiltelefons



8.3 Mögliche Schutzmaßnahmen

M.43 Ende-zu-Ende-Verschlüsselung

Bei der Übertragung von schützenswerten Daten sollte darauf geachtet werden, dass der Übertragungsweg über eine Ende-zu-Ende-Verschlüsselung verfügt. Dies ist nur unter Verwendung von WAP 2.0 gewährleistet. Zur Sicherheit sollte der Anwender den Adressen der Internet-Seiten die Zeichenkette https:// (Hypertext Transfer Protocol Secure) voranstellen und nach erfolgtem Abruf der Internet-Seite das vom Server präsentierte Zertifikat auf Korrektheit überprüfen.

M.44 Schutzmaßnahmen für Aktive Inhalte

Es gelten die im Bereich des Internet üblichen Schutzmaßnahmen beim Zugriff auf Aktive Inhalte.

M.45 Inhalte bestätigen

Mobiltelefon sollten so konfiguriert werden, dass grundsätzlich eine Bestätigung vor dem Herunterladen von Inhalten erforderlich ist.

M.46 Profil löschen

Wenn das WAP-Profil vollständig gelöscht wird, schützt dies vor dem Empfang unerwünschter Push-Nachrichten. Allerdings kann ein Angreifer mittels OTA Provisioning neue Einstellungen auf das Mobiltelefon übertragen.

M.47 Anwenderinteraktion vor Verbindungsherstellung

Mobiltelefone sollten so konfigurieren werden, dass vor dem Aufbau einer Internetverbindung der Anwender gefragt wird, z. B. durch Auswahl eines Internet-Zugangs aus mehreren Möglichkeiten (siehe Abbildung 24). Dann kann der Anwender die

Aktion abbrechen, wenn er nicht sicher ist, dass er den Verbindungsaufbau selber initiiert hatte.

Abbildung 24: Auswahlmenü für Internet-Verbindung

9. Multimedia-Mitteilungen

9.1 Technische Grundlagen

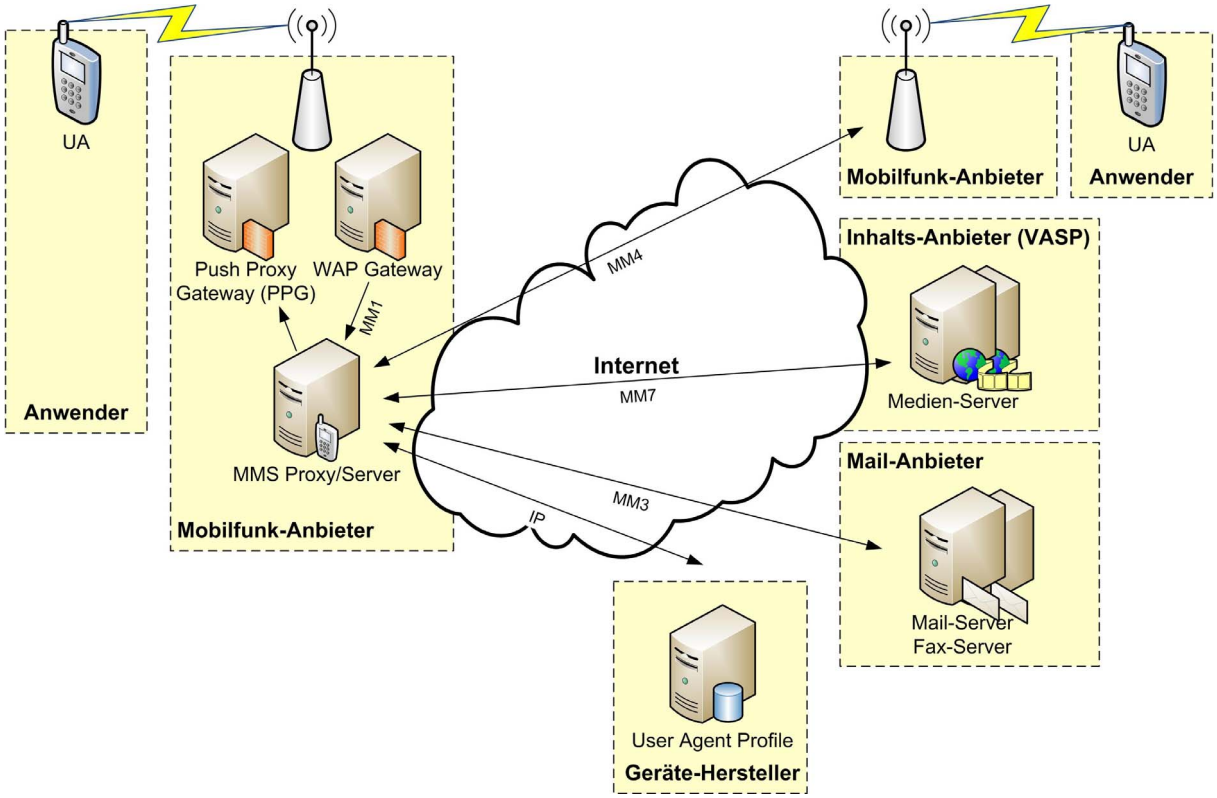
Der Multimedia Messaging Service (MMS) ist in aktuellen Mobilfunknetzen eine Sonderform des WAP (siehe [WAP205]). MMS bietet darüber hinaus zahlreiche Schnittstellen zu anderen Systemen. In der MMS-Referenz-Architektur nach 3GPP werden die Schnittstellen zwischen den einzelnen Komponenten durch die Referenzpunkte MM1 bis MM11 beschrieben. MM3 beschreibt beispielsweise den Referenzpunkt zwischen MMS Proxy/Server und fremden Messaging Systemen wie E-Mail, Fax usw. MM4, MM5 und MM7 stellen weitere Schnittstellen zu Mobilfunkanbieter, Gerätehersteller und Inhaltsanbieter dar. Eine detaillierte Beschreibung von Architektur, Formaten und Schnittstellen findet sich in Publikationen des 3rd Generation Partnership Project (3GPP), z. B. in [3GPP23140].

MMS erlaubt die Übertragung von formatiertem Text und multimedialem Material (Fotos, Videos, Audio) von Mobiltelefon zu Mobiltelefon. Weitere Anwendungsfälle sind die Übertragung solcher Mitteilungen zu Servern im Internet, z. B. als E-Mail oder Telefax, und das Bereitstellen solcher Mitteilungen durch Inhalts-Anbieter im Internet als Value Added Services Provider (VASP). Als Beispiel sei die Übermittlung aktueller (Sport-)Nachrichten inklusive Photos oder Videos an Abonnenten genannt.

Multimedia-Mitteilungen bestehen aus mehreren Teilen (Multipart Message), d. h. Bildern, kurzen Filmen, Tönen, Texten usw.; eine Übersicht der möglichen Formate findet sich in [3GPP26140]. Verbindendes Element ist eine Präsentationssprache. Hierfür kann im Prinzip WML zum Einsatz kommen. Aktuelle Mobiltelefone nutzen jedoch die Synchronised Multimedia Integration Language (SMIL, siehe [SMIL]). SMIL ist eine einfache auf XML-Tags basierende Sprache, die Elemente der Nachricht ordnet, sie in einer bestimmten zeitlichen Reihenfolge darstellt und animiert.

Zentrales Element einer MMS-Architektur ist der MMS Proxy/Server, häufig auch als Multimedia Message Service Center (MMSC) bezeichnet. Das Mobiltelefon kommuniziert mit dem MMS Proxy/Server über das WAP-Gateway. Über diese Schnittstelle, in [3GPP23140] als „Referenzpunkt MM1“ bezeichnet, liefert das Mobiltelefon die Multimedia-Nachrichten ein, die zuvor mit einer separaten Anwendung (MMS Composer) auf dem Telefon zusammengestellt wurde. MM1 verwendet (wie WML) auf der Luftschnittstelle ein effizientes binäres Format (siehe [WAP209]). Das MMSC wertet die in der Nachricht enthaltene Adresse aus und leitet die Nachricht entsprechend weiter. Weitere Schnittstellen sind der „Referenzpunkt MM3“ zum Austausch von Multimedia-Nachrichten mit externen Servern, z.B. für E-Mail und Telefax sowie der „Referenzpunkt MM7“ zum Austausch von Multimedia-Nachrichten mit VASP.

Abbildung 25: MMS-Architektur



Ist als Zieladresse ein Mobiltelefon angegeben, werden die Inhalte der Nachricht durch den MMS Proxy/Server so verändert, dass sie mit dem Zielgerät optimal dargestellt werden können. Es findet dabei i. A. eine Transcodierung der in der Nachricht enthaltenen Bilder, Videos und Töne statt. Zu diesem Zweck erfährt der MMS Proxy/Server den Typ des Mobiltelefons über dessen User Agent Profile (UAProf, siehe Kapitel 8.1.1). Schließlich signalisiert der MMS Proxy/Server dem Mobiltelefon mittels WAP Push das Vorliegen einer Nachricht; die Push-Nachricht enthält einen Verweis (URI), unter dem das Telefon die Multimedia-Nachricht beim MMS Proxy/Server abholen kann (siehe Abbildung 26).

Abbildung 26: Inhalt einer Push-Nachricht für den MMS-Empfang

```
⊟ Encapsulated multipart part:  (application/vnd.wap.mms-message)
    Content-Type: application/vnd.wap.mms-message\r\n
    X-Wap-Application-Id: 4\r\n
    \r\n
  ⊟ MMS Message Encapsulation, Type: m-notification-ind
      X-Mms-Message-Type: m-notification-ind (0x82)
      X-Mms-Transaction-ID: 232
      X-Mms-MMS-Version: 1.0
      From: +4917      63/TYPE=PLMN
      X-Mms-Message-Class: Personal (0x80)
      X-Mms-Message-Size: 3202
      X-Mms-Expiry: 43195.000000000 seconds
      X-Mms-Content-Location: http://       .25/servlets/mms?message-id=232
  Last boundary: \r\n--msgpart_0_1038_1078839587105--
```

Ein Sicherheitsmodell ist für Multimedia-Nachrichten nicht vorgesehen. Es erfolgt insbesondere weder eine Authentisierung des MMS Proxy/Server am Mobiltelefon noch um-

gekehrt. Systeme, die vom Internet auf den MMS Proxy/Server zugreifen wollen, z. B. VASP, müssen sich am MMS Proxy/Server authentisieren. Hierfür werden z. B. die im HTTP definierten Methoden gemäß RFC 2617 verwendet (siehe [RFC2617]).

9.2 Sicherheitsgefährdungen für den Nutzer

G.45 Gefälschte MMS Proxy/Server

Das Fehlen einer Authentisierung des MMS Proxy/Server am Mobiltelefon ermöglicht es einem Angreifer, einen eigenen MMS Proxy/Server zu errichten und damit präparierte Nachrichten an beliebige Mobilfunknutzer zu versenden. Voraussetzung dafür ist, dass die Konfiguration des Mobiltelefons derart geändert wird, dass der vom Angreifer errichtete MMS Proxy/Server benutzt wird. Das kann mittels OTA Provisioning geschehen.

Schutzmaßnahmen siehe M.38

G.46 Aktive Inhalte

Die Ausführung aktiver Inhalte, d. h. nicht sichtbarer Funktionen, die in den empfangenen MMS verborgen sein können, birgt Sicherheitsrisiken, wie beispielsweise die Verbreitung von „Handy-Viren“ und „Handy-Trojanern“. Der Nutzer kann nicht ohne Weiteres erkennen, welche Funktionen sich im Einzelnen in einer MMS verbergen, und hat keine Kontrolle darüber, in welcher Form auf das Endgeräte zugegriffen wird und welche Änderungen möglicherweise vorgenommen werden. Aus der Manipulation von MMS ergibt sich eine Reihe von Gefährdungen.

Schutzmaßnahmen siehe M.47, M.48

G.47 Verbreitung von Handy-Viren

Neben Schnittstellen wie Bluetooth verwenden Handy-Viren häufig MMS als Übertragungsmedium. Hierzu werden infizierte Daten als Teil der aktiven Inhalte für den Anwender unsichtbar einer scheinbar harmlosen MMS angehängt. Steuerbefehle innerhalb der durch SMIL (oder seltener WML) beschriebenen MMS sorgen bei Öffnen für die Ausführung des verseuchten Inhalts, sodass das Endgerät mit dem Schadprogramm infiziert wird. Dies geschieht für den Anwender unsichtbar.

Schutzmaßnahmen siehe M.48, M.49, M.50

G.48 MMS Phishing

Wie auch E-Mail wird MMS für sogenannte Phishing-Attacken genutzt. Phishing setzt sich aus dem englischen password (Passwort) und fishing (Fischen) zusammen. Hierbei wird dem Anwender eine vertrauenswürdige Quelle vorgegaukelt und zur Eingabe persönlicher Daten (z. B. Kontoinformationen) aufgefordert. Durch Aktive Inhalte von MMS werden diese Informationen dann über das Web zum Angreifer übermittelt.

Schutzmaßnahmen siehe M.50, M.51

9.3 Mögliche Schutzmaßnahmen

Da Inhalte von MMS über WAP-Verbindungen eingebunden werden können, gelten hier ebenfalls die in Kapitel 8.3 beschriebenen Schutzmaßnahmen.

M.48 Bestätigen von Downloads

Mobiltelefone sollten so konfiguriert werden, dass eine Bestätigung vor dem Herunterladen von Multimedia-Mitteilungen erforderlich ist.

M.49 Einsatz von Virenschutzprogrammen für mobile Endgeräte

Für eine Vielzahl mobiler Endgeräte sind mittlerweile Virenschutzprogrammene verfügbar. Ein Öffnen von MMS oder anderer Aktiver Inhalte sollte erst nach vorheriger Prüfung auf Schadcode erfolgen, selbst wenn die Quelle vertrauenswürdig erscheint. Darüber hinaus sind eine regelmäßige Prüfung des Endgeräts und die übliche Aktualisierung der Virendefinitionen notwendig.

M.50 Vertrauenswürdige Quellen

Die sicherste Schutzmaßnahme vor dem Schadenspotenzial manipulierte MMS ist der Verzicht auf dieses Medium, falls die gebotenen Funktionen nicht zwingend benötigt werden. Da dies nicht immer möglich oder komfortabel erscheint, muss bei Annahme und Öffnen von MMS mit besonderer Sorgfalt die Identität des Absenders überprüft werden.

M.51 Keine Eingabe persönlicher Daten

Die Aufforderung zur Eingabe von persönlichen Daten sollte generell ignoriert werden. Bei Eintreffen einer solchen Aufforderung aus scheinbar vertrauenswürdiger Quelle sollte der Anwender die Authentizität der Quelle über einen anderen Kanal (zum Beispiel Kontrollanruf) nachprüfen und die angeforderten Daten bei Bedarf über einen alternativen, sicheren Kanal übermitteln (z. B. entsprechend gesichertes Webportal).

10. Anwendungs-Proxys

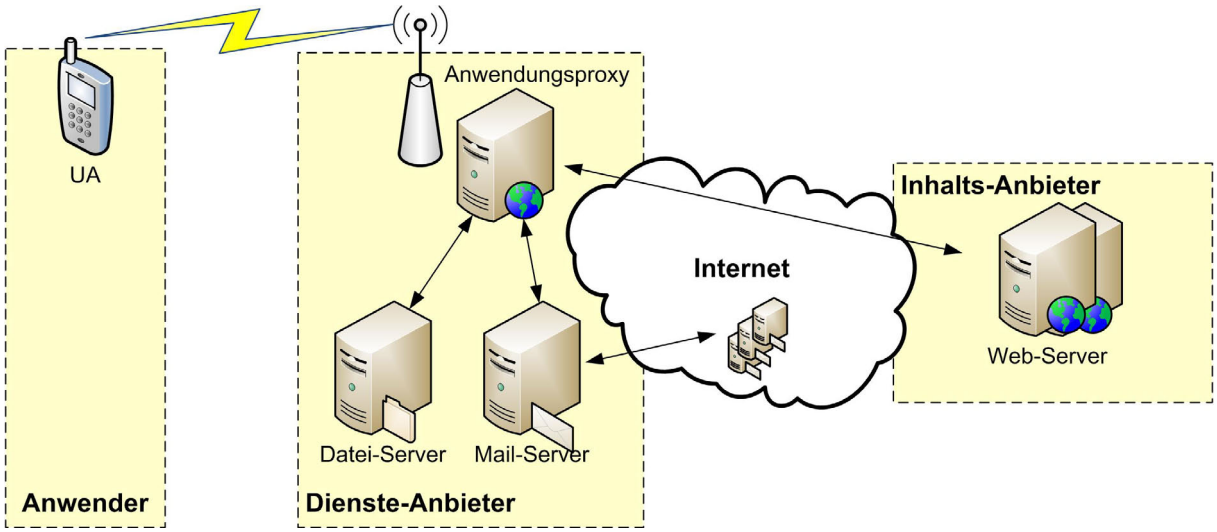
Aufgrund der zunehmenden Verbreitung von internetbasierten Diensten und Informationen ist auch der Zugriff über relativ schmalbandige Mobilfunkverbindungen immer wichtiger geworden. Um die Übertragungskapazität einer Mobilfunkverbindung nicht zu überlasten und Wartezeiten unnötig zu verlängern, ist daher der Einsatz von sogenannten Proxys sinnvoll, die es erlauben, komplexe Inhalte z. B. von Webseiten so aufzubereiten, dass sie erheblich effizienter über Mobilfunk-Verbindungen übertragen werden können. Diese Proxys sind jedoch auch im Hinblick auf Sicherheitsfragen kritisch zu betrachten, sodass im Folgenden darauf eingegangen wird.

10.1 Technische Grundlagen

Verschiedene Anbieter stellen Produkte zum effizienten „Browsen“, zum Empfangen und Versenden von E-Mail, zur Verwaltung von Kalendern und Adressen für Mobiltelefone bereit. Die Produkte werden häufig kostenfrei abgegeben und arbeiten ausschließlich im Zusammenhang mit einem speziellen Proxy beim Anbieter.

Auf dem Mobiltelefon wird zu diesem Zweck eine vom Anbieter zur Verfügung gestellte Software installiert, die auf die Dienste des Proxy zugreift. Dabei werden die vom Proxy aus dem Internet empfangenen Inhalte mittels eines proprietären Protokolls zum Mobiltelefon übertragen und dort dargestellt.

Abbildung 27: Architektur Proxy-basierter Anwendungen für Mobiltelefone



Ziel des Verfahrens ist eine effiziente Übertragung der Inhalte aus dem Internet an das Mobiltelefon. Die Effizienz äußert sich in der erzielten Kompressionsrate. Als Beispiel sei die Proxy-basierte Anzeige der Seite http://www.bsi.de auf einem Mobiltelefon angeführt. Auf einem Standard-Browser benötigte der Aufbau der Seite ca. 150 Kilobyte. Durch Einsatz eines entsprechenden Anwendungs-Proxy wurde die zur Darstellung benötigte Datenmenge auf 25 Kilobyte reduziert. Dabei erfolgt die Darstellung proportional zu der bei einem Standard-Browser gewohnten Ansicht (siehe Abbildung 28). Zur besseren Darstellung auf dem Mobiltelefon lassen sich beliebige Bereiche der Übersicht vergrößern.

Abbildung 28: Vergrößerte Darstellung einer Webseite (Beispiel: Homepage des BSI)

Die genannten AnwendungsProxys erlauben meist eine Verschlüsselung der Daten zwischen Mobiltelefon und Proxy. Eine Ende-zu-Ende-Verschlüsselung bieten die Verfahren jedoch nicht. Insbesondere enden alle z. B. mittels SSL/TLS (Secure Socket Layer/Transport Layer Security) verschlüsselten Verbindungen zu Ressourcen im Internet auf dem Proxy. Einige Anbieter weisen auf diesen Umstand hin und empfehlen Anwendern für die Übertragung vertraulicher Informationen unmittelbar auf dem Mobiltelefon installierte Clients (Browser, E-Mail-Programm) zu verwenden.

Erwähnenswert im Zusammenhang mit den AnwendungsProxys ist die Möglichkeit, persönliche Informationen, wie Lesezeichen, E-Mails, Telefonbücher und Kalendarien auf einem Server beim Anbieter zu hinterlegen. Zu diesem Zweck ist eine Registrierung mit Benutzername und Passwort erforderlich. Die Anbieter bewerben diese Dienste mit der Möglichkeit, Konsistenz der genannten Informationen mit anderen persönlichen Endgeräten, z. B. Personal Computer zu erreichen. Letztlich sind die genannten Dienste mit den im Kapitel 11 beschriebenen Push-Diensten auf Basis eines Network Operation Center (NOC) zu vergleichen, nur richten sie sich vornehmlich an Privatpersonen.

10.2 Sicherheitsgefährdungen für den Nutzer

G.49 Die Vertraulichkeit einer verschlüsselten Verbindung über AnwendungsProxys ist nicht gewährleistet.

Der Proxy ist sowohl aus Sicht des Mobiltelefons als auch aus der Sicht der Anwendung im Internet der Endpunkt des verschlüsselten Kanals. Die Daten passieren den Proxy somit unverschlüsselt. Dadurch ist es einem Angreifer prinzipiell möglich, vertrauliche Informationen auszuspähen, wenn er Zugriff auf den Proxy besitzt.

Schutzmaßnahmen siehe M.52, M.53

G.50 Datenaufzeichnung und Nutzerprofilerstellung

Der Proxy kann dazu verwendet werden, alle von einem Anwender besuchten URL, die dabei erhaltenen Cookies und die von ihm verwendeten E-Mail-Adressen aufzuzeichnen. Auf diese Weise lassen sich Nutzungsprofile für jeden Anwender erstellen.

Schutzmaßnahmen siehe M.52, M.53

G.51 Datenweiterverwertung

Die auf Servern des Anbieters per Synchronisation abgelegten Informationen können durch den Anbieter verwertet werden. So ist z. B. die unerwünschte Vermarktung von Adressen an andere Firmen denkbar, die diese für Werbezwecke benötigen.

Schutzmaßnahmen siehe M.53

10.3 Mögliche Schutzmaßnahmen

M.52 Selektiver Proxy-Einsatz

Auf die Nutzung von AnwendungsProxys für Zugriffe auf vertrauliche Informationen bzw. von Servern im Internet zur Ablage vertraulicher Informationen sollte verzichtet werden.

M.53 Verzicht eines Proxy-Einsatzes

Ein völliger Verzicht auf die Nutzung von AnwendungsProxys bzw. von Servern im Internet als Informationsablage ist zu erwägen.

11. Mobile E-Mail-Synchronisation

Mobile E-Mail-Synchronisation erlaubt das Versenden, Empfangen und Verarbeiten von E-Mail und E-Mail-Anhängen mithilfe mobiler Endgeräte. Der E-Mail-Push-Service übermittelt darüber hinaus dem Anwender seine E-Mails, ähnlich dem Kurzmitteilungs-Dienst (SMS), zeitnah auf sein Mobiltelefon, das über eine Datenverbindung erreichbar ist. E-Mails müssen demnach nicht periodisch oder manuell abgerufen werden, sondern kommen automatisch auf dem mobilen Gerät des Anwenders an. Ebenso werden Termine, Kontakte, Aufgaben und Memos (sogenannte PIM-Daten) sofort synchronisiert. Darüber hinaus ermöglichen Push-Dienste den Zugriff auf unternehmensinterne Datenbanken, wie z. B. Customer Relationship Management Systeme (CRM).

Der Einsatz von mobilen E-Mail-Lösungen ist für viele Anwender interessant, da die Produktivität des einzelnen Mitarbeiters erhöht werden kann. Dieser wird in die Lage versetzt, auch in bisher nicht genutzter Arbeitszeit produktiv zu sein, z. B. in Wartezeiten oder auf Dienstreisen. Die Erreichbarkeit wird ebenso erhöht und die Reaktionszeiten verkürzt. Hierdurch sollen Unternehmensabläufe schneller und effizienter werden.

Die im Folgenden betrachteten Dienste speichern und synchronisieren auf dem mobilen Endgerät die Daten. Diesem Konzept stehen Dienste entgegen, welche die Informationen dem Benutzer online zur Verfügung stellen und daher lokal keine Daten speichern (siehe hierzu Kapitel 10).

Sicherheitsrelevante Aspekte, die sich direkt auf die Endgeräte beziehen, finden sich im Kapitel 14.

11.1 Technische Grundlagen

In einer allgemeinen Betrachtung fallen verschiedene Unterschiede in der Implementierung der mobilen E-Mail-Synchronisation auf. Die technologisch signifikanten Unterscheidungsmerkmale finden sich in der Implementierung der Signalisierung des Endgerätes, der verwendeten Verfahren zur Synchronisation der Daten und in der Infrastruktur des Dienstes.

Bei einem herkömmlichen Client/Server-Modell fragt ein Client nach einem Dienst oder Daten bei einem Server an, welcher die Informationen im Gegenzug übermittelt. Diese Technik wird mit Pull bezeichnet. Im Gegensatz hierzu wird bei einem Push-Dienst keine explizite Anfrage durch den Client vorausgesetzt. Der Server wird von sich aus aktiv, um Daten an den Client zu übertragen. Push-Dienste für mobile Endgeräte werden im Allgemeinen folgendermaßen realisiert:

- Die Synchronisation der Daten wird vom Server durch eine SMS an das mobile Endgerät ausgelöst. Das mobile Endgerät holt sich daraufhin die benötigten Daten vom Server ab. Dieses Verfahren zeichnet sich durch geringen Stromverbrauch aus, da keine Verbindung aufrechterhalten werden muss, während das Endgerät auf eine Signalisierung wartet. Dagegen fallen pro Signalisierung Kosten für die versendete SMS an. Das Verfahren wurde durch die Open Mobile Alliance (OMA) im Rahmen von WAP Push standardisiert und wird durch eine große Anzahl von Endgeräten unterstützt.

- Das mobile Endgerät erhält eine aktive Verbindung zum Server aufrecht. Über diese Verbindung signalisiert der Server den Eingang von Nachrichten. Dieses Verfahren geht in der Regel zu Lasten der Akkulaufzeit. Zusätzlich fallen Kosten für die sogenannten „keep-alive“-Datenpakete an, die benötigt werden, um die Verbindung aktiv zu halten.

Zur Übertragung der Inhalte stellt das Mobilfunknetz dem mobilen Endgerät einen TCP/IP-Zugang zur Verfügung. Hierzu wird beispielsweise GPRS, EDGE oder UMTS genutzt. Darüber hinaus wird, je nach Implementierung, die SMS-Infrastruktur für die Signalisierung verwendet. Die Luftschnittstelle, auf der die Daten zu dem Endgerät übertragen werden entspricht den bei Mobilfunknetzen üblichen Übertragungstechnologien. Je nach eingesetzter Funktechnologie existieren verschiedene Möglichkeiten, diese Verbindung zu schützen. Informationen hierzu finden sich in den Kapiteln 1 bis 5.

Zur eigentlichen Synchronisierung der Daten werden verschiedene Technologien verwendet. Die Open Mobile Alliance (OMA) hat als offenen Standard die SyncML-Protokoll-Familie entwickelt (siehe [OMAsync]), welche die Synchronisation von Daten (Data Synchronisation, DS) und die Verwaltung von Einstellungen (Device Management, DM) erlaubt. Daneben haben verschiedene Hersteller eigene Verfahren entwickelt.

Um eine für die Signalisierung erforderliche Infrastruktur zu realisieren, haben sich zwei Varianten etabliert. Der Unterschied besteht im Wesentlichen darin, ob ein Network Operation Center (NOC) zum Einsatz kommt oder nicht.

11.1.1 Infrastruktur mit NOC

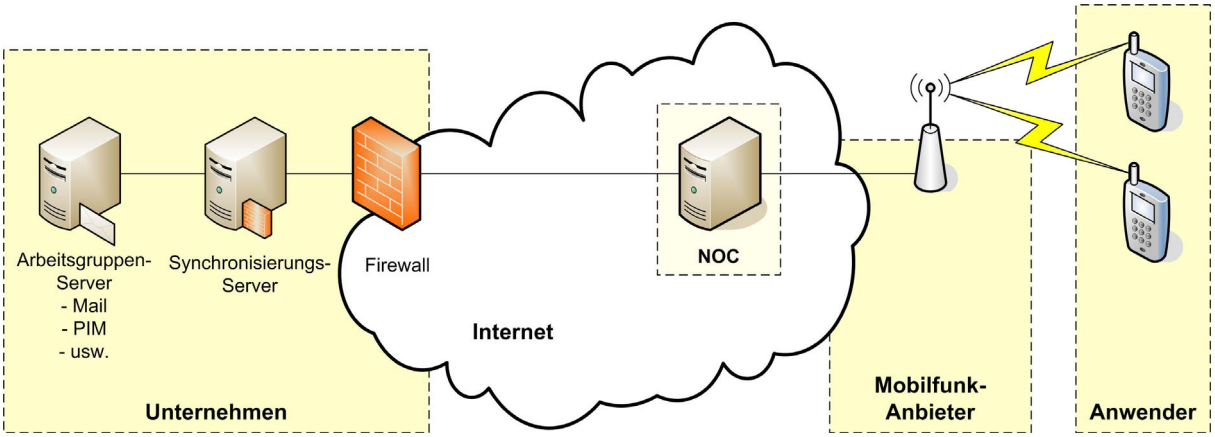
Bei einer Lösung mit NOC (siehe Abbildung 29) erhält der Anwender einen auf das NOC abgestimmten Client. Darüber hinaus stellt das NOC dem Unternehmen eine Server-Komponente zur Verfügung, die als Synchronisations-Server dient oder mit diesem verbunden ist. Dabei ist es unerheblich, ob der Synchronisations-Server als separate Hardware realisiert oder als Software auf dem Arbeitsgruppenserver integriert wurde. Alle Signalisierungs- und Nutzdaten zwischen Unternehmen und den mobilen Endgeräten fließen über das NOC.

Der Synchronisations-Server des Unternehmens teilt dem NOC die Ankunft der E-Mail mit. Das NOC kontaktiert daraufhin das mobile Endgerät über das Mobilfunknetz. Die Übermittlung der E-Mail an das mobile Endgerät kann auf zwei verschiedene Arten realisiert sein:

- Die E-Mail wird zunächst ans NOC geleitet und dort zwischengespeichert. Schließlich übermittelt das NOC die E-Mail an das Endgerät.

- Das NOC stellt einen sicheren Übertragungskanal zwischen mobilem Endgerät und Synchronisations-Server her. Über diesen Kanal wird die E-Mail an das Endgerät übertragen.

Abbildung 29: NOC-basierte Infrastruktur



Der Vorteil der Verwendung eines NOC besteht in der häufig guten Abstimmung der Lösung auf die Fähigkeiten der Mobilfunknetze und der Endgerätebetriebssysteme. Dadurch wird unter anderen eine Optimierung des Clients bezüglich des Stromverbrauchs und der zu übertragenden Datenmenge möglich. Außerdem bieten die Betreiber des NOC zusätzliche Funktionen zur Verwaltung und Absicherung der Endgeräte an, etwa die vollständige Löschung des Endgerätes bei Verlust.

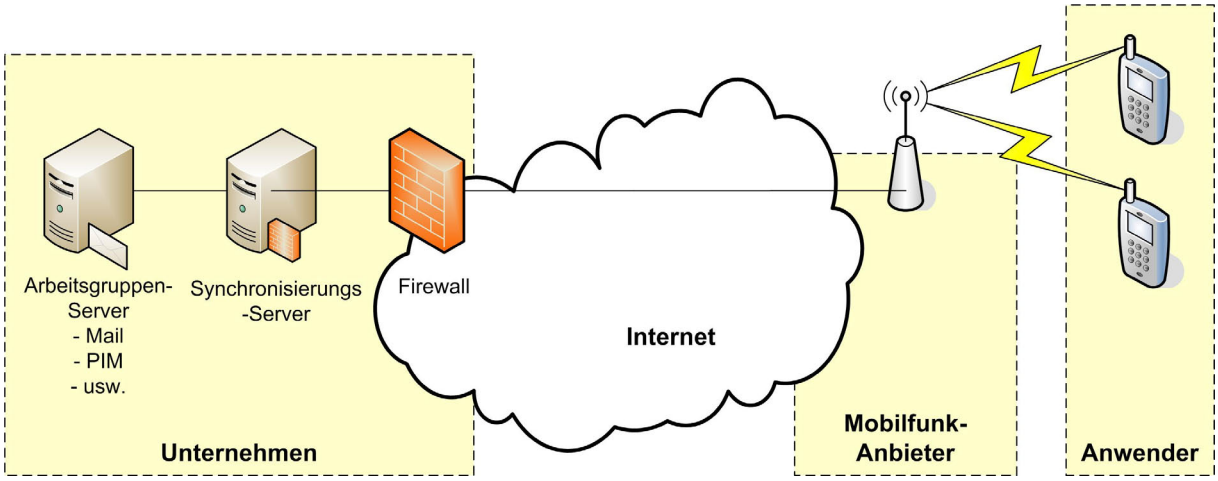
Durch die Einschaltung eines zentralen NOC ergeben sich jedoch auch eine Reihe von Problemen:

- Da alle Daten an die mobilen Endgeräte durch das NOC transportiert werden, muss dem Betreiber des NOC in besonderer Weise vertraut werden.
- Der vom NOC bereitgestellten Serverkomponente ist in besonderer Weise zu vertrauen, da dieser dem Betreiber des NOC eventuell einen Zugriff auf die Firmendaten bietet.
- Ein zentrales NOC kann das Ziel von Denial-of-Service-Angriffen sein. Ein Ausfall des NOC ist gleichzusetzen mit dem Gesamtausfall der Infrastruktur.
- Dem Betreiber des NOC ist es unter Umständen möglich, Bewegungs- und Kommunikationsprofile der Benutzer anzulegen.

11.1.2 Infrastruktur ohne NOC

Als Alternative zum NOC kann die komplette Lösung zur E-Mail-Synchronisation im Unternehmen eingerichtet werden, im Folgenden als Inhouse-Lösung bezeichnet. Der prinzipielle Aufbau einer Inhouse-Lösung wird in Abbildung 30 dargestellt.

Abbildung 30: Infrastruktur ohne NOC



Für die Zustellung einer E-Mail wird kein Vermittler in Form eines NOC verwendet. Somit hat das mobile Endgerät direkten Kontakt mit dem Synchronisations-Server des Unternehmens. Auch hier ist es bezüglich der Funktion unerheblich, ob der Synchronisations-Server als separate Hardware realisiert oder als Software auf dem Arbeitsgruppenserver integriert wurde. Nach Eingang einer E-Mail wird der Synchronisations-Server dem mobilen Endgerät das Eintreffen der E-Mail signalisieren und ihm die Daten senden. Eine Verschlüsselung der Daten erfolgt unmittelbar zwischen Synchronisations-Server und mobilem Endgerät.

Generell stellt sich der Betrieb einer Inhouse-Lösung für ein Unternehmen als aufwendiger dar als ein System mit NOC-Einsatz, da hier die Verwaltung des Synchronisations-Server und der Endgeräte sowie die Pflege der zugehörigen Sicherheits-Infrastruktur vom Unternehmen selbst durchzuführen ist. Es existiert jedoch keine dritte Partei, die Zugriff auf die Daten der Anwender erhält.

Kleine Unternehmen und insbesondere Privatpersonen werden auf den Betrieb einer eigenen Infrastruktur zur E-Mail-Synchronisation häufig ganz verzichten. Sie greifen stattdessen auf Dienste von Unternehmen zurück, die solche Infrastrukturen betreiben und öffentlich anbieten. Der Nutzer bekommt ein E-Mail-Postfach, eine entsprechende Mail-Adresse sowie – falls erforderlich – eine Client-Software für sein mobiles Endgerät. Darüber kann er E-Mails versenden und als Push-Mail empfangen sowie möglicherweise Adressen und Termine synchronisieren. Die Struktur entspricht Abbildung 27; ein Proxy für den Zugriff auf Web-Seiten fehlt jedoch im Allgemeinen.

11.2 Sicherheitsgefährdungen für den Nutzer

G.52 Angriff auf Synchronisations-Server oder Arbeitsgruppenserver über die für die mobilen Endgeräte bzw. für das NOC vorgesehenen Zugänge von außen

Darüber kann Zugriff auf Daten innerhalb des Firmennetzes erlangt werden oder die Firmeninfrastruktur ausgespäht werden. Das Erschleichen einer firmeninternen Identität ist ebenfalls denkbar.

Schutzmaßnahmen siehe M.55, M.56

G.53 Ausspähung der Daten auf den Einrichtungen des NOC

Dieser Angriff kann durch externe Täter, welche ein nicht genügend gesichertes NOC kompromittiert haben, geschehen. Auch Innentäter können nicht ausgeschlossen werden. Die Folge ist eine Offenlegung jeglicher nichtverschlüsselter Kommunikation. Verbindungsdaten und Bewegungsprofile können auf diesem Weg erlangt werden. Auch ist die Erschleichung einer vermeintlich firmeninternen Identität möglich.

Schutzmaßnahmen siehe M.58

G.54 Ausspähen der Daten auf den Einrichtungen eines Anbieters von E-Mail-Diensten im Internet.

Der Angriff kann sowohl durch externe Täter erfolgen, die eine nicht genügend gesicherte Infrastruktur des Anbieters kompromittiert haben, als auch durch Innentäter.

Schutzmaßnahmen siehe M.58, M.52, M.53

G.55 Ausspähen der Daten auf den Übertragungswegen zwischen dem Synchronisations-Server und den mobilen Endgeräten

Hierdurch kann die unverschlüsselte Kommunikation einzelner Teilnehmer ausgespäht werden. Denkbar ist auch eine Manipulation oder Unterdrückung der übertragenen Daten. Ebenso können Kommunikations- und Bewegungsprofile für einzelne Teilnehmer erstellt werden.

Schutzmaßnahmen siehe M.57

G.56 Denial-of-Service-Angriff gegen den Synchronisations-Server

Eine Denial-of-Service-Angriff gegen den Synchronisations-Server kommt einem Gesamtausfall der Infrastruktur gleich und verhindert die Kommunikation zwischen Endgeräten und firmeninternen Datenquellen.

Schutzmaßnahmen siehe M.55

G.57 Denial-of-Service-Angriff auf das NOC

Alle über das NOC angebundenen Datenquellen stehen dem Mobilfunkteilnehmer nicht mehr zur Verfügung.

Keine geeigneten Schutzmaßnahmen möglich

G.58 Zugriff auf das Endgerät

Wird ein mobiles Endgerät verloren oder gestohlen, können Dritte den Speicherinhalt des Gerätes auslesen und an alle dort abgelegten Daten des Nutzers gelangen. Dazu gehören auch Informationen, die einen Zugriff auf das NOC oder den Synchronisations-Server ermöglichen. Auch die Exposition des mobilen Endgerätes im Internet, die durch die Datenverbindung gegeben ist, birgt das Risiko eines Ausspähens von Informationen, die auf dem Endgerät gespeichert sind.

Schutzmaßnahmen siehe M.59, M.60

11.3 Mögliche Schutzmaßnahmen

An dieser Stelle sei zunächst auf das vom BSI veröffentlichte Common Criteria Protection Profile „Mobile Synchronisation Services Protection Profile“ (MSS PP) verwiesen (siehe [BSIMSSPP]). Es nennt als „Target of Evaluation“ (TOE) die Kombination aus Synchronisations-Server, entsprechender Anwendung auf dem Client und der dazwischen liegenden Datenverbindung. Die mögliche Verwendung eines NOC wird im MSS PP berücksichtigt, das NOC selbst ist jedoch nicht Teil des TOE. Das MSS PP geht somit davon aus, dass die Endpunkte einer verschlüsselten Datenverbindung auf Synchronisations-Server und Endgerät liegen. Für den Fall, dass ein NOC eingesetzt wird, fordert das MSS PP einen Betrieb des NOC unter der Verantwortung des Kunden und eine Berücksichtigung des NOC in den Betriebsrichtlinien des Kunden[12].

M.54 Fernadministration der Endgeräte

Die mobilen Endgeräte sollten die Möglichkeit bieten, durch Befehle über die Funkverbindung gesperrt oder gelöscht zu werden. Derartige Funktionen dürfen nur durch vertrauenswürdige Stellen ausgeführt werden können.

M.55 Schutz des Synchronisations-Servers

Der Synchronisations-Server sollte nicht direkt an das Internet angebunden werden, sondern seine Dienste nur über entsprechende Schutzeinrichtungen, z. B. über einen Application Level Gateway anbieten. Dies ist insbesondere wichtig, wenn eine Architektur ohne NOC eingesetzt wird.

M.56 Gegenseitige Authentisierung

Server und Endgeräte sollten sich vor dem Aufbau eines sicheren Kommunikationskanals gegenseitig authentisieren. Beide Kommunikationspartner weisen dazu ihre Identität mithilfe von Zertifikaten nach, die zuvor über sichere Kanäle ausgetauscht wurden.

M.57 Verschlüsselung der Verbindungswege

Eine Verschlüsselung der Datenübertragung ist zwingend notwendig. Sofern die Verschlüsselung nicht bereits von den verwendeten Server- und Client-Komponenten vorgesehen ist, muss eine dienstunabhängige Lösung (z. B. mittels VPN-Tunnel o. ä.) implementiert werden. Ist in die Netzarchitektur ein NOC eingebunden, so muss in jedem Fall die Verbindung zwischen Synchronisations-Server und dem mobilen Endgerät verschlüsselt werden, um das Mitlesen der Informationen im NOC zu verhindern.

M.58 Ende-zu-Ende-Verschlüsselung der E-Mails

Um die vertrauliche Kommunikation zwischen Absender und Empfänger einer E-Mail-Nachricht zu gewährleisten, empfiehlt sich zusätzlich zur Absicherung der Verbindungswege eine Verschlüsselung der E-Mail. Hierzu wird in der Regel zusätz-

[12] „Operating of NOC is explicitly subject to System Operating Policy of the Customer and must be carried out under the general responsibility of the Customer“

liche Software auf dem mobilen Endgerät zu installieren sein, die eine E-Mail-Verschlüsselung ermöglicht.

M.59 Benutzer-Authentisierung am mobilen Endgerät

Um einen Missbrauch der Endgeräte durch Dritte zu verhindern, muss sich der Benutzer am Endgerät authentisieren. Hierfür werden – neben der gewohnten Eingabe von PIN oder Passwörtern – inzwischen auch Verfahren auf Basis von Smartcards oder mittels Biometrischer Merkmale angeboten.

M.60 Datenverschlüsselung auf dem mobilen Endgerät

Die Daten des Nutzers sollten auf dem mobilen Endgerät verschlüsselt abgelegt werden. Die Schlüssel zu deren Entschlüsselung sollten getrennt vom Endgerät aufbewahrt werden, z. B. auf einer Smartcard.

12. M-Commerce Dienste, M-Payment

Im Bereich der mobilen Geschäfte finden sich die unterschiedlichsten Anwendungen. Diese unterscheiden sich stark in Aufmachung, Nutzen und Zielgruppe. Ein bei jeder Anwendung zu findender Aspekt ist die Übertragung per GPRS/UMTS, siehe hierzu Kapitel 2 und 3. Mobile Commerce (M-Commerce) ist mit dem Internet-gestützten Handel (Electronic Commerce, E-Commerce) verwandt. Wie auch im Fall des E-Commerce bilden Netzdienste eine Plattform für Handelstransaktionen zwischen Kunden und Anbietern. Als Abgrenzung zum E-Commerce und Electronic Payment (E-Payment) beziehen sich M-Commerce und M-Payment ausschließlich auf die mobile Nutzung von Handels- und Zahlungsplattformen. Ziel der Technik ist es, durch einen Komfortvorteil auf Seiten des Anwenders dessen Kauflust zu steigern. So soll der Anwender in die Lage versetzt werden, Einkäufe und Bestellungen unterwegs vom mobilen Endgerät aus zu erledigen (M-Commerce) und die notwendigen Zahlungen direkt im Anschluss ebenfalls mobil zu veranlassen. Der Anwender kann - bis dato unverwertbare - Reisezeit effizienter nutzen. Ihm wird dadurch ein Anreiz gegeben, seine Einkäufe beim Anbieter des mobilen Dienstes zu erledigen, statt Bestellungen vom heimischen PC aus oder gar per Post aufzugeben. Auch Dienste wie mobiler Online-Preisvergleich fallen in den Bereich der M-Commerce-Lösungen. Gemeinsam haben alle mobilen Dienste die Verwendung mobiler Sprach- und Datennetze sowie die Optimierung zur Verwendung mit mobilen Endgeräten.

Die verwendete Interaktionstechnik eines solchen Dienstes reicht von Diensten mit Sprachsteuerung (z. B. Fahrplanauskunft) über SMS/MMS gesteuerte Dienste (z. B. Kauf von Klingeltönen) über WAP-basierte Anwendungen (z. B. Internet Banking) bis hin zu komplexen Anwendungen auf dem Endgerät mithilfe von einfachen Scriptsprachen oder höherer Programmiersprachen wie Java. Die Datenübertragung der Anwendungen auf dem Endgerät wird in Push-Dienste und Pull-Dienste kategorisiert. Bei Pull-Diensten initiiert der Benutzer selbst die Datenübertragung vom Dienstanbieter, wobei bei Push-Diensten dieser selbst den Benutzer anspricht. Bei WAP 2.0 wurde das ursprüngliche Sicherheitsprotokoll Wireless Transport Layer Security (WTLS) des WAP-Standards durch die weitverbreitete SSL-Verschlüsselung in Kombination mit HTTP (HTTPS) ersetzt. Den Geschwindigkeitseinbußen durch das nicht speziell für Mobilfunkapplikationen optimierte Protokoll steht gegenüber, dass HTTP als sehr zuverlässig bezüglich der Verschlüsselung und hinreichend sicher für die Übermittlung persönlicher Daten gilt. Durch die weite Verbreitung untersteht der HTTPS-Standard einer ständigen Kontrolle in Bezug auf Sicherheitsmängel durch viele öffentliche und private Stellen. Dies trägt implizit zur Gewährleistung der Qualität und der Aktualität der Verschlüsselungstechnik bei, was einen Vorteil gegenüber der WTLS darstellt. Weitere Informationen zum Thema bietet beispielsweise [HeBuTi40].

12.1 Sicherheitsgefährdungen

Alle M-Commerce Dienste unterliegen den Sicherheitsgefährdungen der jeweiligen Übertragungstechnik. Zusätzlich dazu bestehen je nach Interaktionstechnik weitere Gefährdungen. Diese hängen jedoch stark vom jeweiligen Dienstanbieter und dessen Sicherheitsmechanismen ab. Gefährdete Angriffspunkte sind die Endgeräte sowie die verwendeten Verfahren zur Identifizierung des Kunden (Authentifizierung zu Abrechnungszwecken). Die Abwicklung von elektronischen Bezahlverfahren unterliegt zusätzlich ähnlichen Gefährdungen wie der

E-Commerce (Einkauf oder Dienstleistung per Internet). Zu den hier entstehenden Gefahren sei auf das Informationsangebot des BSI verwiesen (siehe [BSIfB], [BSIEiI]).

G.59 Gefahr der Account-Übernahme durch Abfangen der Zugangsdaten

Sollte es einem Angreifer gelingen, unter Zuhilfenahme einer der jeweiligen Übertragungstechnik eigenen Sicherheitslücke die Zugangsdaten zu geschützten Diensten abzufangen, hat er unter Umständen uneingeschränkten Zugang auf den Dienst. Dies kann je nach Dienst sehr unterschiedliche Folgen für den Betroffenen haben.

Schutzmaßnahmen siehe M.62

G.60 Geldentwendung bei Zahlungsvorgängen

Wenn es ein Angreifer schafft, einen mobilen Zahlungsvorgang abzufangen und es erfolgreich verhindert, dass der eigentliche Zahlungsvorgang ausgeführt wird, so kann er mit der ermittelten Kontonummer, PIN und TAN (Transaktionsnummer) einen neuen Zahlungsvorgang auf ein anderes Konto, mit einem anderen Betrag und einem anderen Betreff vornehmen. Detaillierte Informationen können dem Informationsangebot des BSI-Abschnitt „Online-Banking“ entnommen werden (siehe [BSI-OB]).

Schutzmaßnahmen siehe M.61

G.61 Phishing

Die Folgen der Gefährdungen G.59 und G.60 fallen auch dann in den Möglichkeitsbereich, wenn ein Angreifer durch einen erfolgreichen Phishing-Versuch an die entsprechenden Zugangsdaten kommt. Informationen zu Phishing können dem Informationsangebot des BSI-Abschnitt „Phishing“ entnommen werden (siehe [BSIPh]).

Schutzmaßnahmen siehe M.61, M.63

G.62 Nutzung von M-Commerce in der Öffentlichkeit

Die Nutzung von M-Commerce in der Öffentlichkeit, d. h. dem avisierten Einsatzort, birgt Sicherheitsrisiken. In der Öffentlichkeit können Zugangsdaten zu M-Commerce- und M-Payment-Plattformen bei unachtsamem Umgang mit dem mobilen Endgerät leicht von Dritten ausspioniert werden. Dies stellt ein zusätzliches Risiko im Vergleich zu E-Commerce-Diensten dar, die vom Arbeitsplatz oder dem heimischen PC aus genutzt werden.

Schutzmaßnahmen siehe M.65

12.2 Mögliche Schutzmaßnahmen

Ein wirksamer Schutz gegen etwaige Angriffe speziell auf M-Commerce Anwendungen kann zunächst nur vom Dienstanbieter gewährleistet werden. Hier bleibt es genau zu betrachten, welche Sicherheitsmechanismen der Anbieter nutzt, um z. B. die Datenübertragung zwischen ihm und dem Kunden zu sichern. Effektive Verschlüsselungsmethoden funktionieren nur bei einer Ende-zu-Ende-Verschlüsselung, welche durch Methoden wie SSL zu realisieren ist. Die Verwendung von SSL wird mit dem WAP 2.0-Standard spezifiziert, weshalb Angebote auf Basis von WAP 2.0 zu bevorzugen sind. Um Betrugsversuche ausschließen zu können, sollten

auch die Maßnahmen des Dienstanbieters zur Sicherstellung der Nichtabstreitbarkeit von M-Commerce-Geschäften betrachtet werden.

In Anbetracht der Vielfalt der verschiedenen Dienstanbieter, Übertragungstechniken, Interaktionstechniken und Implementierungen der Dienste gibt es keine allgemeingültige, explizite Schutzmaßnahme. Da jedoch praktisch alle aktuellen Endgeräte mit dem WAP-2.0-Standard kompatibel sind, sollten generell einige Punkte beachtet werden:

M.61 Nur Verbindungen zu vertrauenswürdigen Dienstanbietern aufbauen

Bei der Nutzung von M-Commerce und M-Payment dürfen nur als vertrauenswürdig eingestufte Dienste genutzt werden. Die Bewertung der Vertrauenswürdigkeit kann auf Grundlage von Eigenschaften wie implementierten Sicherheitsstandards, Dauer der Marktpräsenz und Datenschutzbestimmungen (z. B. in den AGBs) vorgenommen werden. Kurzentschlossene Nutzung von neuen oder unbekannten Diensten ohne vorherige Prüfung sollte unbedingt unterlassen werden.

M.62 Nur SSL-verschlüsselte Verbindungen zulassen

Bei der Nutzung von M-Commerce und M-Payment ist als Aspekt der Vertrauenswürdigkeit des Dienstanbieters besonders auf eine Verschlüsselung der Webapplikation zu achten. Diese basiert in der Mehrzahl auf SSL (Adresse beginnt mit https://).

M.63 Nur Kryptografie-taugliche Anwendungen benutzen

Bei der Einstufung der Vertrauenswürdigkeit eines Anbieters ist ein weiteres Kriterium, ob die Applikation eine Ende-zu-Ende-Verschlüsselung erlaubt. Informationen hierzu können gegebenenfalls beim Dienstanbieter eingeholt werden.

M.64 Verwendung sprachgesteuerter Dienste

Sollten nicht alle der oben genannten Schutzmaßnahmen möglich sein, ist die sicherste Interaktionstechnik die Sprachsteuerung. Das Entschlüsseln genormter Tastentöne bei der PIN-Eingabe stellt eine wesentlich leichtere Aufgabe, als das Entschlüsseln von Sprachsignalen dar. Sollten also keine Schutzmaßnahmen möglich sein, wäre die Nutzung von sprachbasierter Authentifizierung vorzuziehen. Hierbei ist aber die Umgebung besonders auf eventuelle Mithörer zu prüfen. Auch das Ausspionieren der Art der vorgenommenen Transaktionen ist mit Kenntnis der Menüstrukturen und dem Abfangen genormter Tastaturtöne ein leichtes. Hier ist die Sprachsteuerung schwerer zu rekonstruieren und damit potenziell sicherer.

M.65 Aufmerksamer Umgang mit Zugangsdaten

Gerade in der Öffentlichkeit muss besonders sorgsam mit Zugangsdaten zu M-Commerce-Diensten umgegangen werden. Von einem Mitführen der Zugangsdaten in schriftlicher Form sowie der Speicherung auf dem mobilen Endgerät ist dringend abzuraten. Vor und während der Eingabe der Daten ist sorgsam zu prüfen, ob sich Dritte in Sichtweite zu Endgeräte-Display und -Tastatur befinden. Zusätzlichen Schutz können Folien bieten, welche auf das Display aufgebracht werden und den Blickwinkel auf das Display minimieren.

13. Location-Based Services

Die Mobilfunknetzbetreiber setzten Anfang dieses Jahrzehnts große Hoffnungen auf standortbezogene Dienste, da sie prinzipiell eine Vielzahl von neuen innovativen Anwendungen ermöglichen. Die Hoffnung der Mobilfunknetzbetreiber war, dass ihre Kunden vermehrt Datendienste nutzen und so mehr Umsatz erzeugen. Standortbezogene Dienste (englisch Location-based Services, LBS) haben im Privatkundenbereich bis heute keinen Durchbruch erzielt. Dennoch bieten alle Netzbetreiber und viele unabhängige Dienstanbieter Anwendungen, die Ortsinformation nutzen. Beispiele für solche Dienste sind:

- Ortung von Freunden oder Kindern
- Flottenmanagement
- Routenplanung, Navigation
- Anzeige von sogenannten Points of Interest in der näheren Umgebung, z. B. Restaurants, Kinos, Geldautomaten und Apotheken

Es ist zudem möglich, dass in Zukunft die Mobilfunknetzbetreiber wie bereits in den USA verpflichtet werden könnten, bei Notrufen auch die Position des Anrufers an die Notrufzentrale zu übermitteln. Damit werden standortbezogene Dienste insgesamt wieder eine größere Aufmerksamkeit erhalten.

13.1 Technische Grundlagen

Standortbezogene Dienste bestehen in der Praxis aus vier Komponenten: Endgerät, Ortungsfunktion, Middleware und Dienstanbieter. Die Endgeräte sind in der Regel Mobiltelefone, können aber auch andere Formen annehmen, wie z. B. Notebooks oder die sogenannte On-Board-Unit bei Mauterfassungs- und Telematiksystemen. Alle hier betrachteten Endgeräte besitzen die Möglichkeit zur drahtlosen Kommunikation, z. B. per GSM oder WLAN (Wireless LAN), und erlauben so einen Zugriff auf ortsabhängige Dienste.[13] Die Ortungsfunktion kann entweder im Endgerät, z. B. in Form eines eingebauten GPS-Empfängers, oder im Netz angesiedelt sein. Bei netzbasierter Ortung wird diese Funktion meist von dem Betreiber der Ortungs- bzw. Kommunikationsinfrastruktur übernommen. Diese Funktion präsentiert die rohen Positionsdaten meist in einer von den angewandten Ortungsverfahren abhängigen Darstellungsform. Die Normierung der Daten und Bereitstellung für Applikationen übernimmt die Middleware, die häufig auch beim Mobilnetzbetreiber angesiedelt ist. Die so aufbereitete Ortinformation wird schließlich von einem Dienstanbieter genutzt und weiterverarbeitet. Dies kann z. B. bedeuten, dass mithilfe einer Datenbank alle Geldautomaten im Umkreis von 200 m ermittelt und per SMS an das Endgerät übertragen werden. Ein weiteres Beispiel wäre die Benachrichtigung von Eltern, falls ihr Kind (bzw. sein Mobiltelefon) außerhalb definierter Gebiete geortet wird.

[13] Reine GPS-Empfänger und andere Geräte ohne Kommunikationsmöglichkeiten werden in dieser Broschüre nicht betrachtet.

Die Schnittstellen zwischen den genannten Komponenten (und ihrer jeweiligen Subsysteme) werden u. a. in den Standards der Open Mobile Alliance (OMA) und des European Telecommunications Standards Institute (ETSI) spezifiziert. Der Standard Mobile Location Server der OMA beschreibt zum Beispiel die Schnittstelle zwischen Ortungsfunktion bzw. Middleware und den Dienstanbietern.

13.1.1 Ortung von mobilen Endgeräten

Im Folgenden werden die grundlegenden Verfahren beschrieben, die zur Ortung von mobilen Endgeräten verwendet werden. Nicht alle Verfahren lassen sich gleich gut auf die gängigen Mobilfunktechnologien GSM und UMTS abbilden bzw. sie können in Abhängigkeit vom zugrunde liegenden System unterschiedlich gute Ergebnisse liefern. Grundsätzlich bietet UMTS jedoch, u. a. durch kleinere Zellgrößen und eine feinere Zeitmessung, bessere Möglichkeiten zur Ortung.

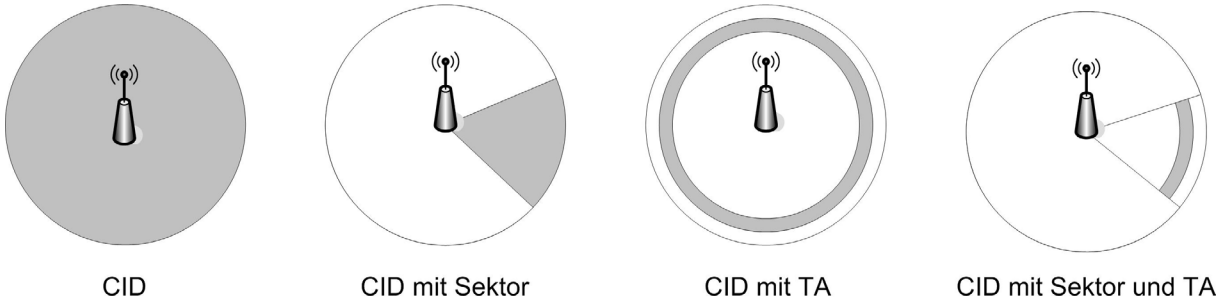
Zellbasierte Verfahren

Die Positionsbestimmung an sich kann technisch betrachtet auf viele Arten umgesetzt werden, die u. a. auch die Genauigkeit der gewonnenen Ortsinformation bestimmen. Die einfachsten Verfahren sind zellbasiert, d. h. sie setzen den Standort des zu ortenden Endgerätes zunächst mit dem Standort der aktuell verwendeten Basisstation gleich. Die Genauigkeit hängt hierbei von der Zellgröße bzw. der Dichte der Basisstationen ab. GSM-Zellen besitzen einen Radius zwischen 100 m und maximal 35 km. Die Genauigkeit dieses Ansatzes kann durch zusätzliche Informationen noch verbessert werden.

- Sektorantennen: Basisstationen sind in der Regel mit gerichteten Antennen ausgestattet, die die Zelle in Sektoren unterteilen. Dies dient eigentlich einer effizienteren Nutzung der vorhandenen Frequenzen, kann jedoch auch die Ortungsgenauigkeit verbessern.

- Timing Advance (TA): GSM verwendet Time Division Multiple Access (TDMA) als Zugangsverfahren, d. h. jedem Endgerät werden dedizierte Zeitintervalle für die Kommunikation zugeteilt. Da sich ein Funksignal mit endlicher Geschwindigkeit ausbreitet, müssen Endgeräte mit zunehmender Entfernung von der Basisstation vor ihrem Zeitintervall mit dem Senden beginnen. Würde dies nicht geschehen, so könnte das Funksignal zu spät an der Basisstation ankommen und in ein Zeitintervall fallen, das einem anderen Endgerät zugeordnet ist. Der zeitliche Versatz, der dies verhindert, wird Timing Advance (TA) genannt und wird in Schritten von rund 3,7 µsec bzw. 550 m angegeben.

Abbildung 31: Zellbasierte Ortungsverfahren



Die sich aus der Kombination von Funkzelle (Cell ID bzw. CID), Sektor und Timing Advance ergebenden sinnvollen Ortungsverfahren sind in Abbildung 31 dargestellt. Auch die Genauigkeit dieser Verfahren hängt stark von der Zellgröße bzw. der Entfernung des Endgerätes von der Basisstation ab. Angenommen, eine Zelle ist in vier Sektoren unterteilt und ein Endgerät befindet sich im Umkreis von 550 m um die Basisstation, so liefert die Kombination aus CID, Sektor und TA eine Fläche von rund 0,24 km² als Ortungsergebnis.

Zu erwähnen ist, dass die Antennendichte auch vom Mobilfunkprovider abhängt. So verfügen nicht alle Anbieter über ein gleichermaßen dichtes Netz von Basisstationen. Während große Provider auch in schwach besiedelten Gebieten eine recht große Anzahl von Basisstationen betreiben, verfügen kleinere Netzbetreiber selbst in städtischen Gebieten oft nur über eine geringe Anzahl. Die bessere Netzabdeckung großer Provider geht daher mit präziseren Ortungsmöglichkeiten einher.

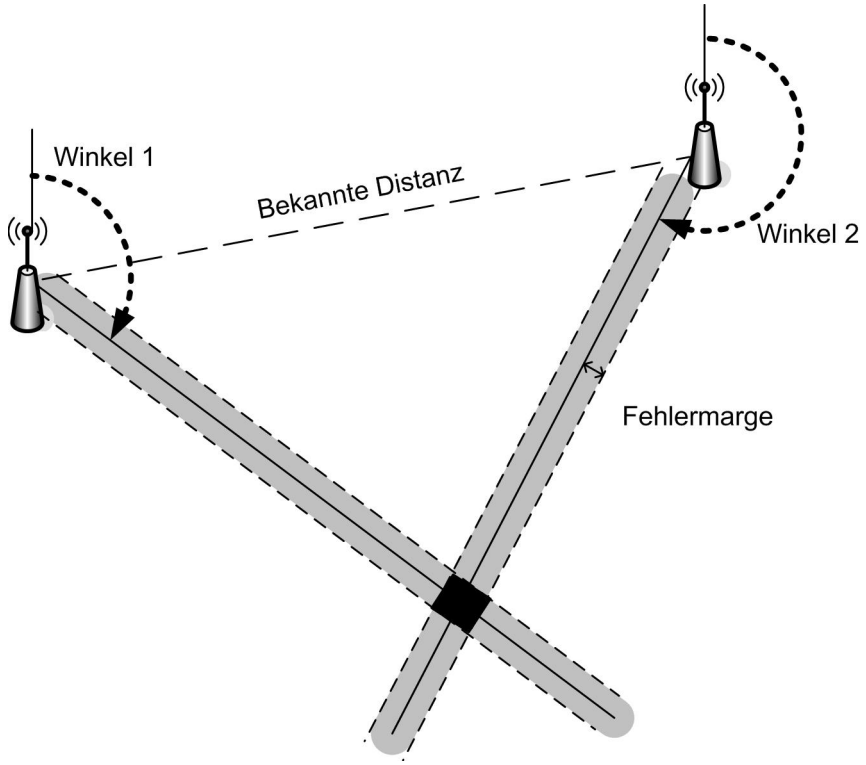
Zeit- und Winkelbasierte Verfahren

Die Ortungsgenauigkeit kann gegenüber einfachen zellbasierten Verfahren erheblich gesteigert werden, wenn Informationen von mehreren benachbarten Zellen zur Verfügung stehen. Als Vorbild für die komplexeren Ortungsverfahren dienen mathematische Methoden, die ursprünglich für die Landvermessung entwickelt wurden. Grundsätzlich lassen sich hier drei verschiedene Ansätze unterscheiden:

- Ortung per Winkelmessung
- Ortung per Distanz- bzw. Signallaufzeitmessung
- Ortung durch Messung von Signallaufzeitdifferenzen

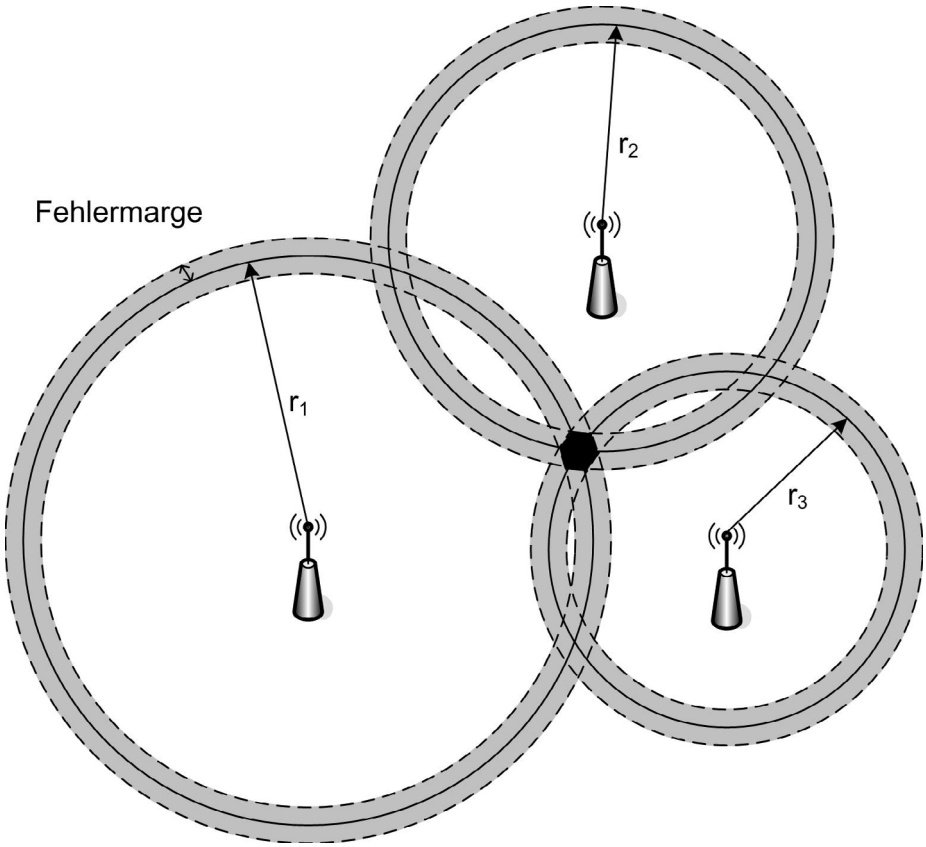
Für die Ortung per Winkelmessung (auch Angulation genannt) werden mindestens zwei Basisstationen mit bekannten Standorten benötigt. (Falls sich das mobile Endgerät zwischen den beiden Basisstationen befindet, wird eine weitere Basisstation benötigt.) Bezüglich dieser Referenzpunkte werden die Winkel zum zu ortenden Mobilfunkgerät gemessen. Die Koordinaten des Geräts entsprechen dem Schnittpunkt der Winkelstrahlen. Dieses in Abbildung 32 dargestellte Verfahren wird häufig in GSM-Netzen mit Sektorantennen verwendet, auch wenn die Antennen nur eine recht grobe Winkelmessung erlauben.

Abbildung 32: Ortung per Winkelmessung (Angulation)



Für die Ortung per Distanzmessung müssen die Entfernungen zu drei Basisstationen mit bekannten Koordinaten zur Verfügung stehen. Dieses wohl bekannteste Verfahren wird auch als Lateration, viel häufiger aber auch fälschlicherweise als Triangulation, bezeichnet. Die Entfernung kann theoretisch über die Signallaufzeiten zwischen dem mobilen Endgerät und den Basisstationen und der Ausbreitungsgeschwindigkeit elektromagnetischer Wellen ermittelt werden. Aus dem Schnittpunkt der Kreise um die Referenzpunkte ergibt sich dann wie in Abbildung 33 gezeigt der Standort des Mobilfunkgerätes. Obwohl dieser Ansatz schnell einleuchtet, stellt sich in der Praxis das Problem der fehlenden gemeinsamen Zeitbasis. Ohne eine hochgenaue zeitliche Synchronisation zwischen Basisstation und Endgerät liefert die Messung der Signallaufzeit nur sehr ungenaue Ergebnisse. Es existieren Vorschläge, dieses Problem zu umgehen, jedoch wird Lateration in der Praxis kaum eingesetzt.

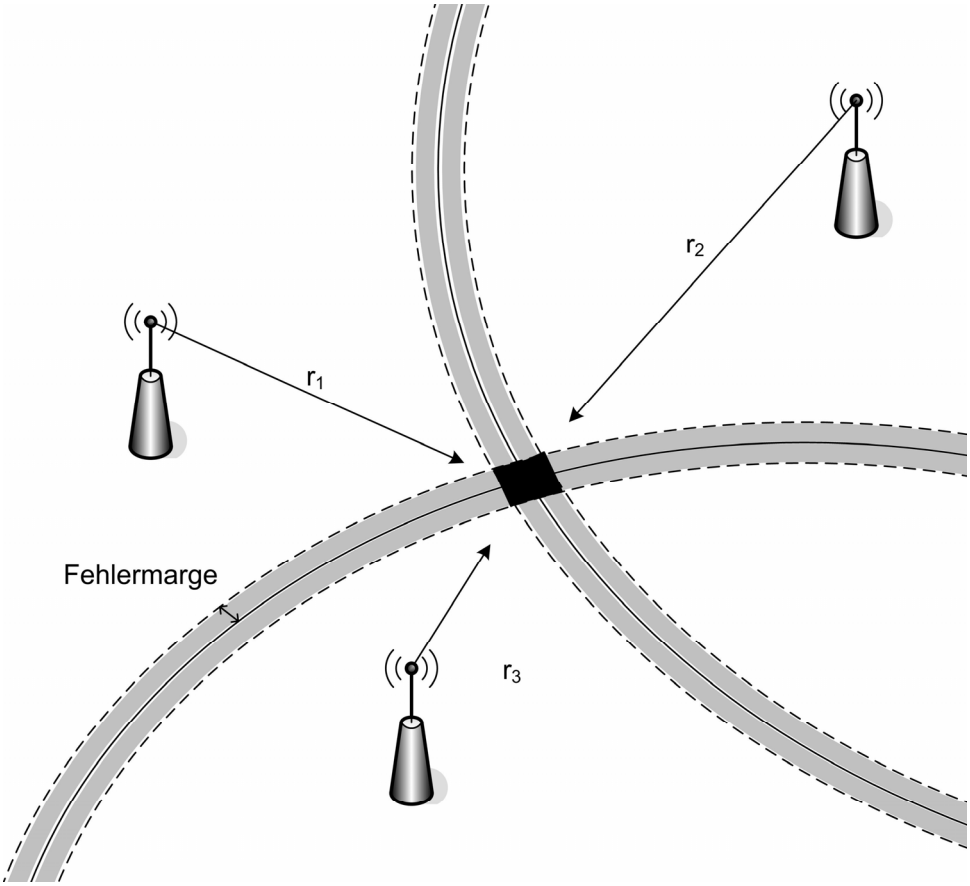
Abbildung 33: Ortung per Zeit- bzw. Distanzmessung (Lateration)



Für die Ortung per Messung der Differenzen von Signallaufzeiten ist hingegen keine Synchronisation zwischen Basisstation und Mobilfunkgerät erforderlich. Lediglich die Basisstationen müssen zeitsynchronisiert sein, was aus technischer Sicht jedoch vergleichsweise einfach durchzuführen ist. Die Signallaufzeitdifferenzen werden gemessen, indem z. B. das mobile Endgerät ein Signal aussendet, das von mindestens drei Basisstationen zu unterschiedlichen Zeitpunkten - abhängig von der Entfernung - empfangen wird. Die Menge der Punkte, für die die Ankunftszeitdifferenz konstant bezüglich eines Basisstationspaars ist, bildet eine Hyperbel. Der Schnittpunkt der Hyperbeln von zwei Paaren von Basisstationen bestimmt dann wie in Abbildung 34 skizziert den Aufenthaltsort des mobilen Endgerätes.

Die Messungen können sowohl am Endgerät als auch an den Basisstationen durchgeführt werden. Alternativ könnten also alle Basisstationen zeitgleich ein Signal aussenden, deren Ankunftszeitdifferenzen am Endgerät gemessen werden. Diese Implementierungsvariante gibt es grundsätzlich auch bei den anderen genannten Ansätzen.

Abbildung 34: Ortung per Zeitdifferenzmessung



In der Literatur werden unterschiedliche Angaben zur Genauigkeit der beschriebenen Verfahren im Kontext von GSM gemacht. Außer von der Zellgröße hängt die Genauigkeit noch von einer Reihe weiterer Faktoren ab. Hierdurch ist eine allgemeingültige Angabe der Genauigkeit weder sinnvoll noch möglich. In der Tat werden konkrete Positionsmessungen in der Regel um einen Fehlerradius entsprechend einer vorgegebenen Wahrscheinlichkeit ergänzt. Die Tabelle gibt daher lediglich grobe Schätzwerte wieder, die aber dennoch ein Bild von den Möglichkeiten der Ortungsverfahren vermitteln. Die in Tabelle 6 enthaltenen Zahlen zum Cell-ID-Verfahren beziehen sich auf eine einzelne Zelle mit einem Radius von einem Kilometer, wie sie typischerweise in Innenstädten anzutreffen ist. In ländlichen Gebieten mit großen Zellradien erhöhen sich die Abweichungen dementsprechend.

Tabelle 6: Genauigkeit der Ortungsverfahren

Verfahren	Genauigkeit	Abhängigkeiten/Besonderheiten
Cell ID	100 m – 1 km Fläche ~ 6,3 km²	Zellgröße, Abweichung bezogen auf Zellposition, weder Richtungs- noch Entfernungsbestimmung
Cell ID mit Sektor	100 m – 1 km (maximaler Fehler; im Mittel weniger) Fläche ~ 6,3 km² /	Zellgröße, Sektorantennen, Abweichung bezogen auf Zellposition, keine Entfernungsmessung, jedoch Richtungseinschränkung

Verfahren	Genauigkeit	Abhängigkeiten/Besonderheiten
	Anzahl Sektoren	
Cell ID mit Timing Advance	100 m – 2 km [14] (im Mittel weniger als Cell ID) Fläche ~ 1,2 km²	Zellgröße, nur Entfernungsmessung, keine Richtungseinschränkung
Cell ID mit Timing Advance und Sektor	75 m – 1,41 km [15] Fläche ~ 1,2 km² / Anzahl der Sektoren	Zellgröße, Zahl der Sektoren, Entfernungsmessung und Einschränkung der Richtung auf einen Sektor
Winkelmessung	50 m – 150 m	Zellgröße, Sektorantennen, Aufrüstung des Netzes, drei Basisstationen
Zeitmessung	50 m – 150 m	Uhrensynchronisation, drei Basisstationen
Zeitdifferenzmessung	50 m – 200 m	Uhrensynchronisation der Basisstationen, drei Basisstationen, entsprechend ausgestattete Endgeräte

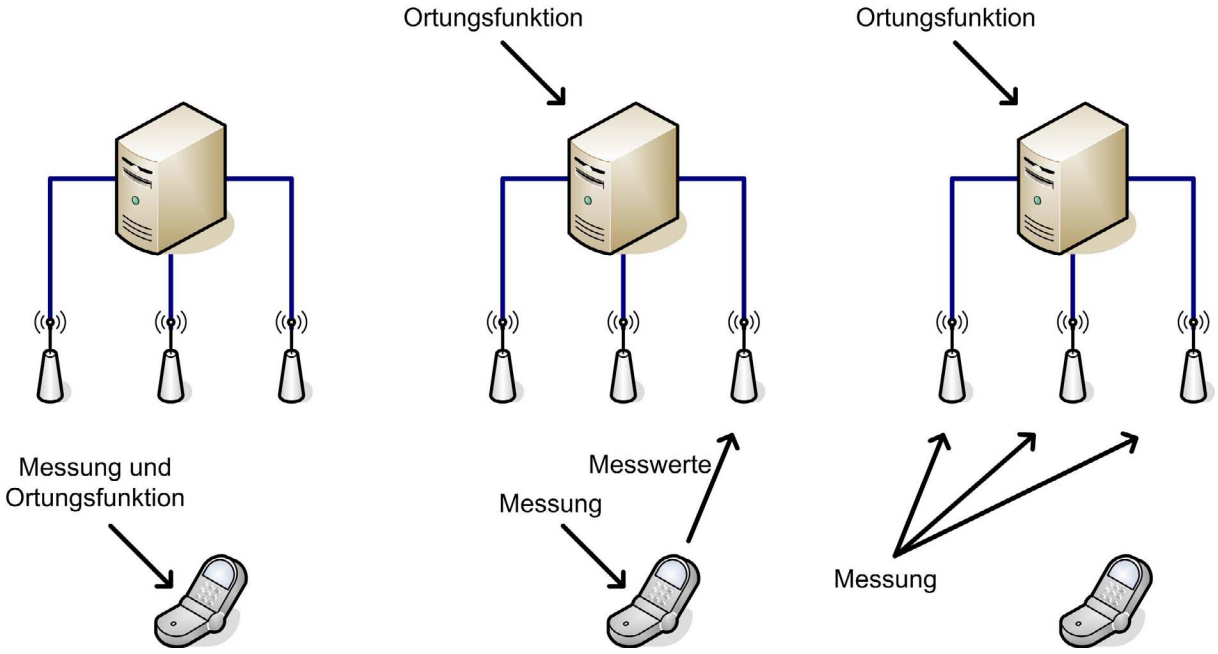
13.1.2 Architekturvarianten

Unter dem Aspekt der Sicherheit ist vornehmlich relevant, wo die Ortungsfunktion angesiedelt und welche Komponenten an der Positionsbestimmung beteiligt sind. Die drei in der Praxis anzutreffenden Varianten sind in Abbildung 35 dargestellt.

[14] Die maximalen Abweichungen beziehen sich auf Ortungen mit nur einer verfügbaren Zelle. In diesem Fall ist keine Richtungsbestimmung bei CID und TA möglich. Die maximale Abweichung beträgt also trotz der Möglichkeit der Entfernungsbestimmung noch 2 km, was dem Worst-Case entspricht. Eine Einschränkung der Richtung bei einer Zelle ist nur mit Sektorierung möglich. Die höhere Genauigkeit spiegelt sich nicht in der konkreten Position, sondern der Einschränkung auf eine Fläche (Ring um Zellmittelpunkt) wider. Diese wurde zusätzlich angegeben.

[15] Dieser Wert ergibt sich aus der maximalen Abweichung innerhalb eines Kreissektors (zugrunde gelegt waren 4 Sektoren als sinnvolle Annahme), also der Sekante zwischen den Sektorrändern. Damit ergibt sich sqrt(2) * radius als maximale Abweichung. Durch die Sektorierung verkleinert sich wiederum die Ergebnisfläche (Sektor eines Kreisrings um Zellmittelpunkt).

Abbildung 35: Verteilung der Ortungs- und Messfunktionen



Die Ortungsfunktion sowie die für die Ortung erforderlichen Messungen können auf dem Endgerät ausgeführt werden. Dies kann z. B. durch einen integrierten GPS-Empfänger erfolgen oder durch spezielle Software, die die Position aus Messungen im Netz berechnet. Die ermittelte Position steht in diesem Fall ausschließlich lokal auf dem georteten Endgerät zur Verfügung. Dies hat den Vorteil, dass der Anwender von Fall zu Fall entscheiden kann, ob er seine Position preisgeben bzw. überhaupt berechnen will.

Da Positionsberechnungen durchaus aufwendig sein können, wird die Ortungsfunktion in einigen Systemen als Teil der Festnetz-Infrastruktur implementiert. Die Messungen werden wie oben beschrieben am Endgerät durchgeführt und dann an die Ortungsfunktion gesendet. Kritisch für den Anwender ist, ob er die Messung unterbinden kann, falls eine Ortung nicht erwünscht ist.

In der letzten Variante sind sowohl die Mess- als auch die Ortungsfunktion in der Netz-Infrastruktur angesiedelt. Hier kann eine Ortung ohne Zutun des Endgeräte-Benutzers durchgeführt werden (siehe auch G.35). Da in Mobilfunknetzen und WLANs die Position des Endgerätes zumindest auf Zellebene bekannt sein muss, bieten die Netze diese Variante mit einer z. B. im Vergleich zu GPS erheblich geringeren Genauigkeit. In Bezug auf ein Mobiltelefon bedeutet dies, dass die einzige Möglichkeit einer Ortung zu entgehen im Ausschalten des Telefons besteht.

13.1.3 Dienste

Die Anzahl der Anbieter solcher Mobiltelefonortungen ist groß und erfreut sich stetigem Wachstum. Um ein Mobiltelefon zur Ortung anzumelden, ist meist nur eine funktionierende E-Mail-Adresse nötig. Nach erfolgreicher Anmeldung muss jedoch das zu ortende Mobiltelefon eingerichtet werden. Hierzu muss bei jedem Anbieter mittels Short Message Service (SMS) eine Bestätigung vom zu ortenden Mobiltelefon zum Dienstanbieter verschickt werden. Danach kann dieses Mobiltelefon beliebig oft geortet werden. Die Anmeldeverfahren variieren sehr stark zwischen den Ortungsanbietern. Bei manchen ist nur die eben genannte

E-Mail-Adresse von Nöten, andere verlangen eine Unterschrift. Es bleibt trotzdem festzuhalten, dass das Orten von Mobiltelefonen ohne die Zustimmung des Besitzers einen Straftatbestand darstellt.

Eine Ortung des Mobiltelefons, ohne dass dieses zumindest kurzzeitig in fremdem Besitz ist, ist ausschließlich den Behörden und Organisationen mit Sicherheitsaufgaben (BOS, zum Beispiel der Polizei) möglich, und das nur mit einer entsprechenden richterlichen Verfügung.

Die Sicherheit des Mobiltelefon-Benutzers hängt vom Anbieter des Ortungsdienstes ab. Einige verschicken nach jeder Ortung eine Benachrichtigung per SMS an das geortete Mobiltelefon, andere informieren in unregelmäßigen Abständen per SMS über die Tatsache, dass dieses Mobiltelefon bei einem Ortungsdienst angemeldet ist. Allerdings existieren auch Anbieter, die eine Konfigurationsmöglichkeit bieten, jedoch nach einer einmal erfolgten Einrichtung keinerlei Hinweise auf eine Ortungsmöglichkeit des Mobiltelefons mehr geben. Dem unerwünschten Übermitteln von Ortungsinformationen kann man dadurch begegnen, dass man per Tastaturkürzel, welches je nach mobilem Endgerät und Provider unterschiedlich implementiert ist, bestimmte Dienste deaktiviert. Das Tastaturkürzel veranlasst das mobile Endgerät dazu, eine Aufforderung an das Providernetz zu übermitteln, welches daraufhin den Dienst providerseitig sperrt.

13.1.4 Datenschutzbestimmungen

Neben den allgemeinen Regelungen im Bundesdatenschutzgesetz (BDSG) existieren weitere Spezialgesetze, in denen Aspekte des Datenschutzes in speziellen Bereichen geregelt werden. Dabei gilt grundsätzlich, dass ein Spezialgesetz Vorrang vor dem allgemeinen Datenschutzrecht besitzt. Im Bereich der Telekommunikation, Tele- und Mediendienste finden im Datenschutz folgende Gesetze Anwendung:

- Telekommunikationsgesetz (TKG)
- Telekommunikationsdatenschutzverordnung (TDSV)
- Teledienstdatenschutzgesetz (TDDSG)
- Teledienstgesetz (TDG)
- Telekommunikationsüberwachungsverordnung (TKÜV)

Diese Gesetze setzen u. a. die entsprechenden europäischen Richtlinien wie z. B. die Richtlinie 2002/58/EG um. Für eine Ortsinformation gilt prinzipiell, dass sie in dem Umfang, der für einen angebotenen Location Based Service nötig ist, verarbeitet werden kann, wenn die Einwilligung des Teilnehmers vorliegt oder die Daten anonymisiert werden. Der Teilnehmer muss vor der Einwilligung von dem Zweck, der Dauer der Speicherung und der möglichen Weitergabe der Daten an Dritte unterrichtet werden. Außerdem muss der Teilnehmer oder Nutzer die Möglichkeit besitzen, jederzeit und unentgeltlich seine Einwilligung zurückzuziehen.

Ab dem 1.1.2009 gilt zudem die sogenannte Vorratsdatenspeicherung, mit der das Kommunikationsverhalten aller Teilnehmer öffentlicher Kommunikationsnetze analysiert werden kann. Für die Speicherung der Telefonverbindungsdaten ist kein Anfangsverdacht erforderlich. Gespeichert werden Rufnummern der Teilnehmer sowie Zeitpunkt und Dauer der Verbindung.

Bei Mobilfunkgesprächen werden zusätzlich die IMEI sowie die verwendeten Funkzellen gespeichert, wodurch sich der Aufenthaltsort ermitteln lässt. Bei Prepaid-Karten wird das Aktivierungsdatum festgehalten. Die Vorratsdatenspeicherung erfasst auch den SMS-Verkehr sowie den Aufbau von Internetverbindungen. Für über das Internet geführte Telefonate werden ebenfalls Zeitpunkt, Dauer und IP-Adressen der Teilnehmer gespeichert. Über die mobile Kommunikation hinaus sind Festnetztelefonie, Internet, E-Mail und Faxverbindungen von der Neuregelung betroffen. Geregelt werden diese Maßnahmen durch das „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ (siehe [DBTtkue]).

13.2 Sicherheitsgefährdungen

G.63 Erstellung von Bewegungsprofilen

Innentäter oder Angreifer, die Zugriff auf Ortungsfunktionen im Providernetz haben, können Bewegungsprofile von Benutzern anlegen. Was von Providern in anonymisierter Form zur Optimierung der Netztopologie durchgeführt wird, könnte unter Kenntnis von IMSI oder IMEI zur Nachverfolgung der Gewohnheiten eines Mobilfunkteilnehmers genutzt werden. Das Spektrum des Missbrauchs reicht vom nichtlegalem Studium von Konsumentengewohnheiten bis hin zur Planung terroristischer oder krimineller Taten.

Schutzmaßnahmen siehe M.66

G.64 Ausnutzen der geografischen Position

Unerlaubtes Auslösen von Ereignissen in Abhängigkeit von der geografischen Position bzw. Nutzung von Ortsinformationen für terroristische Angriffe oder andere Straftaten

Schutzmaßnahmen siehe M.67

13.3 Mögliche Schutzmaßnahmen

M.66 Häufiges Wechseln des Mobiltelefons inklusive SIM-Karte

Ein häufiges Wechseln des Mobiltelefons und der SIM-Karte hilft bei der Verschleierung der Identität eines Mobilfunkteilnehmers. Im privaten Umfeld ist diese Maßnahme meist zu aufwendig und kostspielig. Im geschäftlichen oder institutionellen Umfeld wäre eine Anonymisierung durch Einführung von Endgeräte-Pools möglich. Dies setzt allerdings technische Maßnahmen voraus, um den Nutzer innerhalb der Organisation eindeutig einem Endgerät zuzuordnen und so die Erreichbarkeit sicherzustellen.

M.67 Ausschalten des Mobiltelefons und ggf. Entnahme des Akkus

Falls das Endgerät nicht benötigt wird oder eine Ortung unbedingt vermieden werden muss, ist die wirksamste Maßnahme gegen eine unerwünschte Ortung das Abschalten des Endgerätes. Da sich einige Endgeräte nicht vollständig stromlos schalten lassen und eventuell auch im Stand-by-Modus noch zu orten sind, empfiehlt sich im Zweifelsfall die Entnahme des Akkus aus dem Endgerät.

14. Hardware und allgemeine Sicherheitsfragen

Es kommt heute eine große Bandbreite von mobilen Endgeräten zum Einsatz. Dies können mobile Endgeräte sein, die hauptsächlich im Privatanwenderbereich eingesetzt werden, wie etwa mobile Musik- oder Videoplayer. Im privaten, aber besonders auch im geschäftlichen Umfeld finden darüber hinaus eine Reihe von mobilen Endgeräten mit Anbindung an Mobilfunknetze Verwendung, hauptsächlich Mobiltelefone, Handheldcomputer, Notebooks sowie eine Reihe von Spezialgeräten, beispielsweise im medizinischen Sektor.

Die in diesem Abschnitt geschilderten Sicherheitsbedrohungen beziehen sich ausschließlich auf den Bereich der Endgeräte mit Einsatz in Mobilfunknetzen, sogenannte Mobile Stations (MS), auch wenn ein Teil der Sicherheitsbedrohungen auch auf andere Bereiche übertragbar ist. Für eine Übersicht über die Sicherheitsbedrohungen und Schutzmaßnahmen für mobile Endgeräte im Allgemeinen sei auf die Broschüre - „Mobile Endgeräte und mobile Applikationen – Sicherheitsgefährdungen und Schutzmaßnahmen“ des Bundesamtes für Sicherheit in der Informationstechnik verwiesen (siehe [BSIMoEMoA]).

Auf Seiten der Hardware bieten sich bei mobilen Endgeräten einige besondere Sicherheitsbedrohungen. Durch die kompakte Bauform ist es z. B. unmöglich, beschädigte oder veraltete Komponenten auszutauschen. Daher ist es dem Nutzer auch nicht möglich, das entsprechende Gerät zu öffnen, um es auf Manipulationen zu untersuchen. Angreifern mit entsprechender Fachkenntnis und Werkzeugen ist es jedoch ein Leichtes, die Geräte zur Manipulation zu öffnen. Des Weiteren ergeben sich aus typischen Schnittstellen – etwa für Erweiterungskarten oder den Austausch von Daten – weitere Ansatzpunkte für eine Manipulation.

14.1 Sicherheitsgefährdungen

Im Folgenden werden Sicherheitsbedrohungen beschrieben, die für mobile Endgeräte durch ihre Beschaffenheit und ihre Verwendung entstehen können. Diese gliedern sich in allgemeingültige Sicherheitsbedrohungen, Bedrohungen durch Beschaffenheit der Hardware und Gefährdungen durch die eingesetzte Software. Im Anschluss finden sich mögliche Schutzmaßnahmen.

G.65 Diebstahl

Durch die Kompaktheit der heutigen Endgeräte besteht eine besonders hohe Gefahr des Diebstahls. Der physikalische Zugriff auf ein Endgerät erleichtert es einem potenziellen Angreifer deutlich, Informationen und Daten zu erbeuten.

Schutzmaßnahmen siehe M.68, M.71

G.66 Unzureichende Geheimhaltung der PIN

Zumeist werden mobile Endgeräte in einem öffentlichen Umfeld eingesetzt. Die Sicherung des Mobiltelefons erfolgt zumeist über einen Zahlencode (Personal Identification Number, PIN). Die Eingabe dieser PIN in öffentlichem Raum stellt eine potenzielle Gefahr dar, da ein Angreifer die PIN leicht unbemerkt ausspionieren könnte und, sobald er das Endgerät in Händen hält, Zugriff auf das mobile Endgerät erlangt.

Der Diebstahl eines Endgerätes und der PIN ermöglicht zum einen den Zugriff auf persönliche und geschäftliche Daten, die auf dem Endgerät gespeichert sind. Da die im Endgerät enthaltene SIM-Karte (Subscriber Identity Module) die digitale Identität des Benutzers gegenüber dem Mobilfunk-Anbieter darstellt, ist zum anderen durch die Übernahme des Endgerätes die Übernahme der Identität des Besitzers möglich. So kann der Angreifer im Namen des Endgerätebenutzers Vertragsverhältnisse eingehen oder andere betrügerische Handlungen begehen.

Schutzmaßnahmen siehe M.69

G.67 Verleih des Endgerätes

Der kurzzeitige Verleih von Endgeräten zur Verwendung mit einer anderen SIM-Karte, z. B. aus Hilfsbereitschaft aus einer vermeintlichen Notsituation heraus, ist als kritisch einzustufen. Zwar werden oftmals personenbezogene Daten wie Telefonnummern, SMS und andere Kontaktdaten auf der persönlichen SIM-Karte gespeichert. Jedoch ist dies abhängig vom verwendeten mobilen Endgerät und der Speicherkapazität der SIM. Somit sind viele personenbezogene Daten auch unter Verwendung einer fremden SIM-Karte auf dem Endgerät zugreifbar. Gleiches gilt auch im umgekehrten Fall, sodass nach Rückgabe eventuell auf dem Endgerät verbliebene Daten ausgelesen werden können.

Schutzmaßnahmen siehe M.70, M.71

G.68 Manipulation der Hardware

Manipulation von Hardware kann zum Ausfall des Gerätes führen. Des Weiteren kann manipulierte Hardware zum Auslesen von persönlichen Daten und Kontakten genutzt werden.

Schutzmaßnahmen siehe M.5, M.73, M.75

G.69 Anbringung von Abhöreinrichtungen

Abhöreinrichtungen sind durch die heute mögliche Miniaturisierung problemlos in ein Mobiltelefon zu integrieren. Selbst für Privatpersonen sind Mikrofon-Sender-Kombinationen mit deutlich unter 10 mm Kantenlänge erhältlich. Austauschbare Zierschalen sind einfach zu demontieren und bieten oftmals Hohlräume, die sich zum Verbergen von Abhöreinrichtungen eignen.

Schutzmaßnahmen siehe M.5, M.74, M.75

G.70 Datendiebstahl durch Entwenden von Speicherkarten

Durch die Erweiterung mobiler Endgeräte um speicherintensive Funktionen (wie z. B. MP3-Player, Kameras usw.) erfreuen sich Speicherkarten zunehmender Beliebtheit. Diese werden in einem ins Endgerät integrierten Kartenleser eingelegt. Aus Komfortgründen sind diese meist leicht zugänglich, sodass es für einen Angreifer ein Leichtes ist, die Speicherkarte in einem unbeobachteten Moment zu entwenden. Weil diese Speicherkarten gängigen Standards (wie z. B. Micro SD oder Multimedia Card, MMC) entsprechen, sind kompatible Lesegeräte flächendeckend verfügbar. Unverschlüsselt auf Speicherkarten abgelegte Informationen können so problemlos ausgelesen werden.

Schutzmaßnahmen siehe M.76, M.77

G.71 Zugriff auf Daten über Datenkabel für Synchronisation (Mail, Kontakte usw.). Zugriff über Bluetooth siehe Kapitel 15.

Personen im Besitz des Endgeräts können über Datenkabel die auf dem Endgerät gespeicherten Informationen auslesen (Synchronisierung). Darunter fallen persönliche Nachrichten und Kontakte. Der Zugriff per Datenkabel setzt den Besitz der Endgeräte-PIN voraus.

Schutzmaßnahmen siehe M.78, M.79

14.2 Mögliche Schutzmaßnahmen

M.68 Transport und Aufbewahrung von mobilen Endgeräten in verschließbaren Taschen. Kein Zurücklassen von Mobiltelefonen in nicht sicheren Räumen

Mobile Endgeräte sollten nicht unbeobachtet zurückgelassen werden (öffentlich zugängliche Räume, Kfz usw.). Neben der Diebstahlgefahr erhöht dies die Gefahr der unbemerkten Manipulation von Endgeräten und des Datendiebstahls.

M.69 Aufmerksamer Umgang mit mobilen Endgeräten in der Öffentlichkeit

Bei Benutzung von mobilen Endgeräten in der Öffentlichkeit empfiehlt sich ein sorgsamer Umgang mit sensiblen Daten. Insbesondere sollte die Eingabe der PIN nur unter Sichtschutz gegenüber anderen Personen stattfinden.

M.70 Verleih von Endgeräten nur an absolut vertrauenswürdige Personen, nach Möglichkeit kein Verleih des Mobiltelefons

Endgeräte mit sensiblen Daten sollten im Regelfall nicht verliehen werden. Falls unausweichlich, sollte ein Verleih nur an als absolut vertrauenswürdig eingestufte Personen stattfinden.

M.71 Speicherung personenbezogener Daten – falls technisch möglich – nur auf SIM-Karte

Bei Verleih des Endgerätes sollte beachtet werden, dass sensible Daten nur auf der SIM-Karte gespeichert werden, soweit dies technisch möglich ist. Der telefoninterne Speicher sollte nur verschlüsselt genutzt werden sowie eventuell verwendete Speicherkarten (z. B. Smart-Cards) und SIM-Karten vor dem Verleih entnommen werden. Dies schützt sensible Daten auch bei Verlust des Endgeräts.

M.72 Schutz des Endgerätes mit einem Passwort

Die Wahl eines Passwortes für das Endgerät sichert es zuverlässig gegen unbefugten Zugriff. Manche Endgeräte erfordern bei Wechsel der SIM-Karte die Eingabe des Endgerätepassworts. Dies erhöht den Schutz gegen unbefugten Zugriff auf Daten und die Weiterverwendung des Endgeräts.

M.73 Versiegelung entsprechender Verschlüsse und Verschraubungen nach Kauf des Gerätes

Eine Versieglung von Schrauben, Clips und anderen Verschlussmechanismen - beispielsweise mit Spezialfarben – verhindert die unbemerkte Manipulation und die Anbringung von Abhöreinrichtungen.

M.74 Verzicht auf mobile Endgeräte mit austauschbaren Zierschalen

Der Verzicht auf mobile Endgeräte mit austauschbaren Zierschalen erschwert die Anbringung von Abhöreinrichtungen. Falls doch Endgeräte mit Zierschalen eingesetzt werden, sollten die Montagevorrichtungen für die Schalen nach M.73 behandelt werden.

M.75 Untersuchung auf Hardwaremanipulation

Die Untersuchung von Endgeräten auf Manipulation ist technisch aufwendig und entsprechend kostspielig. Trotzdem lohnt sich dieser Aufwand in besonders schützenswerten Einsatzgebieten. Eine Möglichkeit ist die Untersuchung mittels Röntgenprüfgeräten. Ähnlich der Durchleuchtung des Handgepäcks am Flughafen können so elektronische Geräte berührungsfrei auf Manipulation untersucht werden.

M.76 Verzicht auf Speicherkarten oder auf Speicherung von vertraulichen Daten auf Speicherkarten

Ein Datendiebstahl kann bei Einsatz von Speicherkarten auf verschiedene Weise verhindert werden. Der komplette Verzicht auf Speicherkarten kann eine Lösung sein, ist aber nicht immer möglich. Daher empfiehlt sich der Verzicht einer Speicherung sensibler Daten auf entnehmbaren Speicherkarten.

M.77 Verschlüsselung der auf Speicherkarten und im internen Speicher abgelegten Daten

Ist der Verzicht auf Speicherkarten nicht möglich oder nicht erwünscht, so ist eine starke Verschlüsselung der abgelegten Daten notwendig. Dies wird bereits von vielen Endgeräten unterstützt. Ebenso sollten auch die Daten im internen Speicher der Endgeräte verschlüsselt abgelegt sein.

M.78 Schutz der Synchronisationsschnittstelle mit PIN oder Passwort, sorgsamer Umgang mit PIN

Falls die Synchronisierungsschnittstelle genutzt werden soll, so müssen Authentifizierungsmechanismen für diese Schnittstelle aktiviert werden. Dies kann zum Beispiel eine PIN oder Passwortabfrage sein. Eine Speicherung der Anmeldeinformationen auf dem zu synchronisierenden Arbeitsplatzrechner ist nicht empfehlenswert.

M.79 Abschaltung der Synchronisationsschnittstelle

Falls generell oder über längere Zeit die Synchronisierungsschnittstelle nicht genutzt wird, empfiehlt es sich diese per Konfiguration zu deaktivieren. Eine solche Möglichkeit ist nicht immer vorhanden.

15. Kommunikationsschnittstellen

Mobile Endgeräte verfügen heutzutage über unterschiedliche Schnittstellen und Möglichkeiten, um Peripherie anzuschließen und die Kommunikation mit anderen Geräten zu ermöglichen.

Im Folgenden soll nur exemplarisch auf die häufig genutzte Bluetooth-Schnittstelle eingegangen werden. Daneben existieren noch andere Schnittstellen wie WLAN oder IrDA (Infrared Data Association). Hier gelten ähnliche Sicherheitsbedrohungen, auf die aber im Einzelnen nicht mehr explizit eingegangen werden soll.

Nähere Informationen hierzu finden sich in „Drahtlose lokale Kommunikationssysteme und ihre Sicherheitsaspekte“ der Local-Wireless-Communication-Gruppe des BSI (siehe [BSIDlKSa]).

Als zukunftsträchtige Kommunikationsmöglichkeiten wird im Weiteren auch auf die bisher im Zusammenhang mit mobilen Endgeräten noch kaum verbreitete Nutzung von RFID (Radio Frequency Identification) eingegangen.

15.1 Bluetooth

Bluetooth ist ein Funkstandard, der zur Verbindung von mobilen Geräten dient. Er liegt mittlerweile in Version 2.1 vor, welcher allerdings noch von keinem Endgerät implementiert wird. Mit der Version 2.0 wurde die Datenrate von rund 700 kbit/s auf 2,1 Mbit/s angehoben (Enhanced Data Rate, EDR). Da jedoch die große Mehrzahl der Endgeräte derzeit noch Bluetooth 1.2 unterstützt und sich die Version 2.0 erst langsam durchsetzt, beziehen sich die Aussagen in diesem Dokument auf Version 1.2 des Standards. Für detaillierte Informationen zu diesem Thema sei auf „Drahtlose lokale Kommunikationssysteme und ihre Sicherheitsaspekte“ der Local-Wireless-Communication-Gruppe des BSI hingewiesen (siehe [BSIDlKSa]).

Die Übertragung findet auf dem ISM-Band (Industrial-Science-Medical, 2,4 GHz) statt. Bluetooth benötigt keinen Sichtkontakt zwischen den Geräten und hat eine Reichweite von 10 bis 100 m. Grundsätzlich bietet ein Mobiltelefon drei verschiedene Bluetooth-Modi:

- Bluetooth an, Gerät sichtbar
- Bluetooth an, Gerät nicht sichtbar
- Bluetooth aus

Die von Bluetooth verwendete Authentifizierung ist einseitig, weshalb die Durchführung einer Man-In-The-Middle-Attacke möglich ist. Eine sichere Verbindung kann nur durch Verschlüsselung aufgebaut werden. Diese Funktionalität ist jedoch optional und muss von einem der Teilnehmer angefordert werden. Die Verschlüsselung erfolgt entweder auf Basis eines Kombinationsschlüssels oder eines Geräteschlüssels. Die Verschlüsselung anhand des statischen Geräteschlüssels ist allerdings generell nicht empfehlenswert.

Größte Neuerung in Bluetooth Version 2.1 ist das sogenannte Secure Simple Pairing. Dieses Verfahren ergänzt das bisherige, durch eine zu schwach gewählte PIN potenziell anfällige

Verschlüsselungsverfahren. Hierbei wird keine vorab durch den Anwender gewählte PIN genutzt. Stattdessen wird bei Verbindungsaufbau auf Basis eines Public Key Verfahrens auf beiden Endgeräten ein Schlüssel errechnet. Ist das Ergebnis auf beiden Geräten identisch, ist der verschlüsselte Kanal nicht kompromittiert. Der Anwender bestätigt nun auf beiden Geräten die Richtigkeit des Schlüssels und die Verbindung ist hergestellt. Neben der manuellen Bestätigung existieren noch weitere Methoden zur Verifikation. Eine ist der Abgleich des Schlüssels über einen alternativen Kommunikationskanal. Hierfür kann beispielsweise auf die RFID-basierte Near-Field-Communication (NFC) zurückgegriffen werden. Durch Secure Simple Pairing sollen die Schwächen des herkömmlichen PIN-basierten Verfahrens behoben und Man-in-the-Middle-Attacken unterbunden werden.

15.1.1 Sicherheitsgefährdungen

G.72 Man-In-The-Middle-Attacke

Wurde von keinem Bluetooth-Teilnehmer eine Verschlüsselung der Verbindung angefordert, kann ein Angreifer alle zwischen den beiden Geräten übertragenen Daten abfangen und anhand der Gerätenummern dechiffrieren.

Schutzmaßnahmen siehe M.80

G.73 Verwendung wenig komplexer PINs

Sollten die Bluetooth-Teilnehmer eine Verschlüsselung anhand von Combination Keys angefordert haben, aber wenig komplexe PINs verwenden, ist auch hier ein Abfangen der Kommunikation möglich. So können diese PINs durch Mitschnitt des Verbindungsaufbaus erraten werden. Für 7-stellige Ziffernkombinationen ist dies innerhalb von 77 Sekunden möglich.

Schutzmaßnahmen siehe M.81

Tabelle 7: Durch das BSI empfohlene PIN-Längen bei vorgegebenem Zeichensatz

Verwendete Zeichen	Min. empfohlene PIN-Länge	Minimale PIN-Länge
0-9 (10 Zeichen)	19 Stellen (= 63 Bit)	12 Stellen (= 40 Bit)
0-9, A-Z (36 Zeichen)	12 Stellen (= 62 Bit)	8 Stellen (= 41 Bit)
0-9, A-Z, a-z (62 Zeichen)	11 Stellen (= 65 Bit)	7 Stellen (= 42 Bit)
(druckbares) ASCII (95 Zeichen)	10 Stellen (= 66 Bit)	6 Stellen (= 39 Bit)

G.74 Bluetooth-Tracking

Sollte Bluetooth eingeschaltet sein, ist es möglich, die Position des Geräts zu orten. Hierzu werden mehrere Bluetooth-Empfänger benötigt, die idealerweise über empfangsverstärkende Modifikationen verfügen. Es sind bereits Beispiele vorhanden, in denen, mit entsprechendem Equipment, Reichweiten jenseits der Zwei-Kilometer-Marke erreicht wurden. Je nach Art der Ausstattung der Angreifer spielt es hierbei auch keine Rolle, ob das Gerät als sichtbar oder unsichtbar konfiguriert wurde.

Schutzmaßnahmen siehe M.82

G.75 Bluetooth-Hacking-Software

Es besteht die Möglichkeit, aus verschiedenen Quellen spezielle Hacking-Software für Bluetooth-Geräte, insbesondere für Handys zu beziehen. Diese Programme liegen in verschiedener Form vor, von Linux-Programmen mit leistungsstarken Empfangseinheiten zur Verwendung für Massen-Hacks bis hin zu Java-Applets für Javafähige Handys. Die Verwundbarkeit eines Endgeräts hängt stark vom eingebauten Bluetooth-Standard und dem Gerät selbst ab. So ist das Hacken von älteren Handymodellen bestimmter Hersteller zuweilen einfacher als das Hacken von aktuellen Modellen. Die Möglichkeiten der verschiedenen Programme sind z. B.:

- Lahmlegen des Endgeräts (DoS-Attacke)
- Auslesen und Modifizieren von Daten im Gerätespeicher (z. B. Telefonbuch, SMS-Speicher, E-Mail-Speicher, Daten auf der Speicherkarte usw.)
- Konfiguration des Endgeräts (Lautlosschalten, Rufannahme, Weiterleitung, Anrufe tätigen, zu einer Telefonkonferenz einladen usw.)

Ein gehacktes Mobiltelefon kann vom Angreifer komplett konfiguriert und ferngesteuert werden. Die hierbei gewonnenen Daten und möglichen Modifikationen erlauben es dem Angreifer ebenfalls, später mit anderen Geräten eine automatisch konfigurierte Bluetooth-Verbindung aufzubauen. Ebenfalls können so die Verbindungsdaten für Datenverbindungen geändert werden, um z. B. über einen vom Angreifer kontrollierten Proxy umzuleiten, auf dem alle übertragenen Daten gespeichert und später vom Angreifer ausgewertet werden können.

Schutzmaßnahmen siehe M.83

G.76 Optionale Verschlüsselung

Die Verschlüsselung von Bluetooth ist optional. Dass dem Anwender die Verschlüsselung freigestellt wird, stellt eine zusätzliche Gefährdung der übertragenen Daten dar.

Schutzmaßnahmen siehe M.80

15.1.2 Mögliche Schutzmaßnahmen

M.80 Anforderung von Verschlüsselung

Es sollte bei jeder Verbindung grundsätzlich eine Verschlüsselung angefordert werden. Unverschlüsselte Verbindungsversuche sollten grundsätzlich abgelehnt werden.

M.81 Komplexe Bluetooth-PIN

Die für die erfolgreiche Verbindung der Geräte auf beiden Seiten einzugebende Bluetooth-PIN muss so komplex wie möglich ausfallen. Hierbei können theoretisch, abhängig vom Endgerät, nicht nur Zahlen genutzt werden. Es sollten möglichst starke PINs mit Zahlen, Großbuchstaben, Kleinbuchstaben und Sonderzeichen verwendet werden.

M.82 Schutz vor Bluetooth-Tracking

Um ein Bluetooth-Tracking effektiv verhindern zu können, muss die Bluetooth-Funktionalität des Endgeräts deaktiviert werden. Ist dies nicht immer möglich, reicht

es nicht, das Gerät auf unsichtbar zu schalten. Auch in diesem Modus kann mit entsprechender Hardware die Gerätenummer (Bluetooth-ID) ausgelesen und das Opfer identifiziert werden. Sollte Bluetooth also aktiviert bleiben müssen, bietet nur der stetige Wechsel der Gerätenummer einen wirksamen Schutz vor Angreifern. Hieraus ergeben sich jedoch Nachteile für die Bedienbarkeit der an das entsprechende Gerät anzuschließenden anderen Bluetooth-Geräte. Ändert sich die Gerätenummer des Gerätes, muss ein erneutes Pairing mit allen verwendeten Bluetooth-Geräten durchgeführt werden.

M.83 Schutz vor Hacking-Software

Wie in vielen anderen Bereichen wird auch hier ein stetiger Vorteilswechsel von Angreifern und Verteidigern erfolgen. Es sollten Endgeräte verwendet werden, die die Möglichkeit bieten, Dienstanwendungen wie Firewall und Viren-Scanner zu nutzen. Es gelten ebenfalls die Schutzmaßnamen M.76 bis M.82.

15.2 Radio-Frequency Identification

Langfristig ist die Ausstattung von mobilen Endgeräten mit Radio-Frequency Identification (RFID) zu erwarten. Daher soll hier ein kurzer Überblick über diese Technik und ihre sicherheitsrelevanten Aspekte gegeben werden. Für detaillierte Informationen sei auf das Papier „Risiken und Chancen des Einsatzes von RFID-Systemen“ des BSI verwiesen (siehe [BSIRFID]).

RFID bezeichnet einen Standard, der zur Kennzeichnung und Nachverfolgung von Gegenständen und Waren auf Basis von Funktechnologie entwickelt wurde. Bereits heute existieren mobile Endgeräte, die über Lesegeräte für RFID verfügen. Die Zahl dieser Geräte dürfte in Zukunft zunehmen, da sich durch RFID viele Identifikationsprozesse lösen lassen. Neben der Identifizierung und Lokalisierung von Gegenständen steht RFID auch für die automatische Erfassung und Speicherung von Daten.

Die Kommunikation mit RFID-Transpondern erfolgt berührungslos und erfordert keinen direkten Sichtkontakt. Ein RFID-System besteht aus drei unterschiedlichen Komponenten:

- RFID-Transponder (auch: Tags) speichern eine eindeutige Identifikationsnummer und weitere Daten.
- Lesegeräte ermöglichen eine Kommunikation mit den Tags, d. h. das Lesen und Schreiben der Daten.
- IT-Systeme sorgen für eine Weiterverarbeitung der Daten. Beispiele hierfür sind Zugangskontroll- und Lagerwirtschaftssysteme.

Auf dem Markt ist eine Vielzahl höchst unterschiedlicher Transponder für unterschiedlichste Anwendungen erhältlich. In vielen Branchen gehört die Nutzung von RFID-Technologie inzwischen zum Standard, beispielsweise das Gesundheitswesen, das Transportwesen und die Logistik. Funktionen wie Zutrittskontrolle, Arbeitsplatz- und Raumbuchung sowie Desk-Sharing-Umgebungen werden ebenfalls zunehmend auf Basis einer RFID-Infrastruktur implementiert.

Eine Anwendung von RFID für mobile Endgeräte, die sich in naher Zukunft etablieren könnte, wird derzeit in mehreren Pilotprojekten evaluiert. Beispielsweise wird ein mit RFID-Leser ausgestattetes Mobiltelefon zum Lösen von Tickets im ÖPNV (Öffentlicher Personennahverkehr) eingesetzt. Per RFID werden vom Anwender Informationen wie Terminalkennung, Buchungszeitpunkt, Start- und Zielbahnhof aus dem Terminal ausgelesen. Ein weiteres Einsatzfeld für RFID ist der Schlüssel-Abgleich nach Bluetooth Version 2.1 (Secure Simple Pairing). Wenn sich solche Verfahren etablieren, ist es absehbar, dass in Zukunft Mobiltelefone vermehrt mit RFID-Lesegeräten ausgestattet sein werden.

15.2.1 Sicherheitsgefährdungen

G.77 Erstellung von Bewegungsprofilen

Aktive RFID-Transponder sind über eine Entfernung von einigen hundert Metern lokalisierbar. Aber auch passive RFID-Tags können auf kurze Entfernung ausgelesen werden. Des Weiteren lassen sich die zugehörigen Lesegeräte ebenfalls während eines Lesevorgangs orten. Sind nun vermehrt mobile Endgeräte mit RFID-Technologie ausgestattet, ließen sich mit entsprechender Technik Bewegungsprofile von Anwendern erstellen. Dies kann nutzbringend eingesetzt werden, z. B. zur Ortung von medizinischen Notfällen, aber auch missbräuchlich, etwa zu Marktforschungszwecken.

Schutzmaßnahmen siehe M.84, M.85, M.86

G.78 Ausspähen persönlicher Gegenstände

Durch die zunehmende Kennzeichnung von Waren mit RFID-Tags nimmt auch die Gefahr zu, dass diese Transponder ausgelesen werden, um so Kenntnis über persönliche Gegenstände von Personen zu erlangen. Die denkbaren Missbrauchsformen sind auch hier vielfältig und reichen von individualisierten Werbeangeboten bis hin zur Analyse von persönlichen Gewohnheiten.

Schutzmaßnahmen siehe M.84, M.85, M.86

G.79 Unerlaubte Veränderung bzw. Manipulation der Tag-Daten

Insbesondere ältere und kostengünstige Modelle von RFID-Transpondern senden sämtliche Daten inkl. ID im Klartext. Während neuere Standards auch beidseitige Authentifizierungsverfahren unterstützen, ist es bei einfachen Transpondern möglich, dessen Identität zu übernehmen und falsche oder manipulierte Daten anstelle des originalen RFID-Tags auszusenden. Dadurch ist die Datensicherheit RFID-basierter Systeme nicht mehr gewährleistet, was in industriellen Prozessen oder Authentisierungs-Verfahren unabsehbare Folgen haben kann. Ein mögliches Beispiel wäre die Übernahme der Identität eines Anwenders, der sich an seinem Mobilen Endgerät mittels RFID-Tag authentifiziert.

Schutzmaßnahmen siehe M.87

15.2.2 Mögliche Schutzmaßnahmen

M.84 Entfernen unerwünschter Tags

Unerwünschte RFID-Transponder sollten nach Möglichkeit entfernt werden. Oftmals ist eine Entfernung jedoch nicht möglich, da der Transponder bereits herstellerseitig verbaut oder – z. B. im Falle von Warensicherungssystemen – bewusst an unzugänglichen Stellen des Gegenstands angebracht wurde.

M.85 Abschirmen

Eine elektromagnetische Abschirmung von aktiven und passiven Funksendern ist prinzipiell immer möglich, sodass auch nicht entfernbare RFID-Tags abgeschirmt werden können. Jedoch stellt sich oftmals die Frage nach der Realisierbarkeit, da etwa mobile Endgeräte ebenfalls Funktechnologien nutzen und eine Abschirmung sie ihrer Funktion berauben würde. Eine lokalisierte Abschirmung des RFID-Tags ist hingegen vermutlich aufwendiger als die Entfernung desselben.

M.86 Störsender

Der Einsatz von Störsendern für die Betriebsfrequenzen von RFID ist eine denkbare Lösung für sicherheitskritische Bereiche. Ein flächendeckender Einsatz ist jedoch teuer und meist nicht realisierbar. Der Einsatz eines transportablen Störsenders (englisch jammer) ist für die meisten Frequenzbereiche im deutschen Rechtsraum untersagt, da eine Beeinträchtigung anderer technischer Einrichtungen und eine Störung anderer Frequenzbänder nicht ausgeschlossen werden kann.

M.87 Schutz der Tag-Daten vor Veränderungen

Beim Einsatz von RFID-Technik in sicherheitskritischen Systemen ist möglichst auf RFID-Tags ohne Möglichkeiten zur beidseitigen Authentifizierung und Verschlüsselung zu verzichten. Auch von Transpondern, die zur Manipulation ihres Datenspeichers keine Authentifizierung verlangen, ist dringend abzuraten.

16. Software

Die auf mobilen Endgeräten eingesetzte Software unterliegt denselben Bedrohungen wie andere Arten von Software auch. Die darüber hinausgehenden Bedrohungslagen gliedern sich in drei Gruppen:

- von Firmware und Betriebssystem ausgehend
- durch Anwender-Applikationen hervorgerufen
- durch Schadprogramme ausgelöst

16.1 Firmware und Konfiguration

Für die Firmware und auf dem Endgerät gespeicherte Konfigurationsdaten ergeben sich einige Sicherheitsbedrohungen. Diese ergeben sich aus Techniken, die von Seiten der Provider zur Umsetzung von erzwungenen Standardkonfigurationen und Serviceangeboten genutzt werden. Prominente Beispiele hierfür sind OTA und SIM-Toolkit.

Die unter dem Begriff OTA Programming bekannte Technik wird mittlerweile von vielen, jedoch nicht allen Mobilfunkherstellern unterstützt. OTA wird, wie auch ihre Derivate OTAPA (OTA Parameter Administration), OTAP (OTA Provisioning) und OTASP (OTA Service Provisioning) von vielen Providern eingesetzt. Während OTAP und OTASP zu Abrechnungszwecken eingesetzt werden, bieten OTA und OTAPA dem Provider die Möglichkeit, ohne Beteiligung des Nutzers Konfigurationsdaten des mobilen Endgeräts anzupassen und Applikationen zu installieren. Dies erleichtert das zentrale Management der mobilen Endgeräte und die Einhaltung eventuell vertraglich festgehaltener Betriebsparameter für Endgeräte.

Die seit 1999 gebräuchlichen SIM-Karten erlauben die Speicherung von kleinen Programmen, die per SMS auf die SIM-Karte übertragen werden können. Diese ebenfalls von Mobilfunk-Anbietern genutzte Technik namens SIM-Toolkit ermöglicht das Speichern von geräteunabhängigen Applikationen auf der durch den Provider zur Verfügung gestellten SIM-Karte. Provider nutzen dies für anbieterspezifische Dienste (z. B. Homezone) und für die Umsetzung von Informationsdiensten.

16.1.1 Sicherheitsgefährdungen

G.80 Over-The-Air Programming (OTA)

Einem potenziellen Angreifer ermöglicht diese Technik die Manipulation der Konfigurationsdaten derart, dass das manipulierte Gerät den Betrieb verweigert, was einer DoS-Attacke (Denial-of-Service) auf Endgeräteseite entspricht.

Keine geeigneten Schutzmaßnahmen möglich

G.81 Proxy-Manipulation

Eine weitere denkbare Manipulation per OTA Programming erlaubt die Einstellung eines fremden Proxy für die Datenübertragung. So würde – vom Anwender un-

bemerkt – sämtlicher Datenverkehr über einen feindlichen Proxy umgeleitet und könnte somit abgehört und rekonstruiert werden.

Keine geeigneten Schutzmaßnahmen möglich

G.82 FOTA – Firmware Over The Air

FOTA bezeichnet eine weitere Technik aus der OTA-Gruppe. Sie erlaubt das Einspielen von Firmware Updates durch den Provider. Das Einspielen manipulierter Firmware könnte als Grundlage für nahezu beliebige Folgeangriffe dienen.

Keine geeigneten Schutzmaßnahmen möglich

G.83 SIM-Toolkit

SIM-Applikationen könnten so manipuliert sein, dass sie das Auslesen von sicherheitsrelevanten Daten sowie das Abhören von Telefongesprächen erlauben.

Keine geeigneten Schutzmaßnahmen möglich

G.84 Automatische Rufannahme

Die meisten Mobiltelefone unterstützen eine automatische Rufannahme. Dies ist eine konfigurierbare Einstellung, wodurch ein Mobiltelefon selbständig einen eingehenden Anruf ohne weiteres Zutun des Besitzers entgegennimmt. Hierbei kann in der Regel noch die Anzahl der Rufzeichen vorgewählt werden, nach der die automatische Rufannahme erfolgen soll. Diese Option kann sinnvoll sein, wenn beispielsweise das Mobiltelefon mit Headset im Auto ohne Freisprecheinrichtung genutzt werden soll.

Riskant ist dies jedoch z. B. in Besprechungen, wenn das Mobiltelefon auf lautlos geschaltet ist. So kann unbemerkt ein Anruf entgegengenommen werden, wodurch das Mobiltelefon als Abhöreinrichtung fungieren kann. Automatisch angenommene Marketing-Anrufe können im Falle von Roaming auch bei angerufenen Teilnehmern hohe Kosten verursachen.

Gegenmaßnamen siehe M.88

16.1.2 Mögliche Schutzmaßnahmen

Gegen die Verwendung von OTA und verwandten Techniken sowie Service-SMS und SIM-Toolkit durch den Provider kann der Kunde kaum Gegenmaßnahmen ergreifen. Wünschenswert wäre, dass die Betriebssysteme der Endgeräte die Manipulation von Konfigurationsdaten von außen nur auf ausdrückliche Betätigung des Anwenders hin zulassen.

M.88 Abschaltung der automatischen Rufannahme

Eine automatische Rufannahme sollte vorrangig deaktiviert werden. Man sollte sie nur dann konfigurieren, wenn sie tatsächlich benötigt wird (z. B. im Auto ohne Freisprecheinrichtung, nur mit Headset).

16.2 Applikationen

Da heutige mobile Endgeräte über einen, wenn auch eingeschränkten, so doch ähnlichen Funktionsumfang verfügen wie Arbeitsplatzrechner, wird auch eine zunehmende Zahl von Applikationen auf ihnen ausgeführt. Diese können unterschiedlichster Natur sein und reichen von Adressverwaltung über Tabellenkalkulation bis hin zu Instant Messaging und anderen Kommunikationsanwendungen. Die hohe Anzahl der installierten Applikationen und der damit einhergehenden Verlust der Übersichtlichkeit erleichtert das Verstecken von Schadprogrammen (siehe dazu Kapitel 16.3).

Ein großer Teil mobiler Applikationen nutzt Dienste im öffentlichen oder privaten Mobilfunknetz. Die hierdurch entstehenden Sicherheitsbedrohungen und eventuelle Gegenmaßnahmen sind in Kapitel 6 geschildert. Jedoch entstehen über die von Netzdiensten ausgehenden Sicherheitsbedrohungen hinaus weitere Gefährdungen durch den bloßen Einsatz solcher Software.

16.2.1 Sicherheitsgefährdungen

G.85 Eingeschränkte Wahlfreiheit

Die Entscheidung für eine bestimmte Software zieht möglicherweise den zwingenden Einsatz eines bestimmten mobilen Betriebssystems nach sich. Durch diese eingeschränkte Wahlmöglichkeit nimmt man sämtliche mit einem bestimmten Betriebssystem verbundenen Sicherheitsmängel in Kauf.

Schutzmaßnahmen siehe M.89

G.86 Mangelnde Implementierung von Sicherheitsmechanismen

Die Applikation implementiert die Verwaltung und Speicherung personenbezogener oder sicherheitsrelevanter Daten nicht entsprechend heutigen Sicherheitsstandards. Dadurch können nachgeschaltete Schutzmechanismen, etwa der verwendeten Netz-Dienste, kompromittiert werden und somit ihre Wirksamkeit verlieren. Außerdem wird beim Anwender ein falsches Sicherheitsgefühl ausgelöst, der sich auf angeblich vorhandene Sicherungsmechanismen verlässt.

Schutzmaßnahmen siehe M.90

16.2.2 Mögliche Schutzmaßnahmen

M.89 Prüfung von Software-Abhängigkeiten

Vor der Entscheidung für den Einsatz einer bestimmten Applikation muss die Bindung an bestimmte Betriebssysteme geprüft werden. Sind für diese Betriebssysteme Sicherheitsmängel bekannt oder bestehen sonstige Bedenken über die Integrität der Betriebssysteme, ist eine Evaluierung bestehender Alternativ-Applikationen notwendig.

M.90 Einfordern von Sicherheitszertifizierungen

Vor dem Einsatz einer Applikation wird geprüft, ob der Hersteller entsprechende Sicherheitszertifizierungen vorweisen kann oder ob Studien die korrekte Implementierung belegen. Ist dies nicht der Fall, so sollte eine alternative Applikation eingesetzt

werden. Falls Alternativen nicht vorhanden sind, sollten bekannte Sicherheitsmängel der Software evaluiert werden und eventuell von einem Einsatz abgesehen werden.

M.91 Applikationsvielfalt beschränken

Die Zahl der eingesetzten Applikationen sollte auf das benötigte Minimum beschränkt werden, da so die Zahl der insgesamt vorhandenen Sicherheitsrisiken eingegrenzt werden kann, ohne konkrete technische Maßnahmen einleiten zu müssen.

16.3 Schadprogramme

Mit zunehmendem Funktionsumfang der Betriebssysteme mobiler Endgeräte nimmt auch die Gefahr durch Schadprogramme zu. Zwar existiert noch nicht eine solche Vielzahl wie im Bereich der Personal Computer; erste Varianten wurden aber bereits entdeckt und ihre Zahl steigt stetig. Man unterscheidet zwei verschiedene Grundformen bezüglich der Verbreitung Während Viren sich durch die Weitergabe von scheinbar vertrauenswürdigen, infizierten Dateien verbreiten, pflanzen sich Würmer selbstständig über Netze fort. Hierzu kommen Dienste wie E-Mail, MMS (Multimedia Messaging Service) oder sogar SMS zum Einsatz.

Bislang sind lediglich Viren bekannt, bei deren Installation der Nutzer mitwirken muss. Dies geschieht durch eine Eingabeaufforderung zur Ausführung aktiven Inhalts in MMS. Würmer, die zum Beispiel die sogenannte Service-SMS (SIM-Toolkit) als Verbreitungsweg nutzen, sind denkbar, aber bislang nicht nachgewiesen.

16.3.1 Sicherheitsgefährdungen

G.87 DoS durch Viren

Die Infektion durch Viren kann zum Ausfall des Geräts führen, was einer DoS-Attacke gleichkommt. Auch der Verlust sensibler Daten ist möglich. Als Beispiel sei ComWarrior genannt, der erste bekannte MMS-Virus mit nennenswerter Verbreitung.

Schutzmaßnahmen siehe M.92, M.93, M.94

G.88 Verbindungskosten durch Würmer

Die Verbreitung von Würmern bindet Netzressourcen und könnte somit die Funktionalität von mobilen Endgeräten einschränken. Die entstehenden Verbindungskosten wären nicht kontrollierbar.

Schutzmaßnahmen siehe M.92, M.93, M.94

G.89 Trojanisches Pferd

Schadprogramme können eine Hintertürfunktion enthalten. Diese Trojanischen Pferde oder auch Trojaner genannte Form der Schadprogramme erlaubt Angreifern den Zugriff auf System und Daten. So können etwa Verbindungsdaten protokolliert werden oder das Handy als Abhöreinrichtung genutzt werden.

Schutzmaßnahmen siehe M.92, M.93, M.94

G.90 Kommerzielle Überwachungssoftware

Unabhängig von Viren und Würmern existieren weitere Formen von Trojanischen Pferden, sogar kommerzielle Varianten, welche dem Anwender ermöglichen, ein fremdes Mobilfunkgerät auszuspionieren oder es als Abhörgerät zu missbrauchen. Dazu müssen diese Programme durch den Angreifer auf dem Endgerät installiert werden. Danach protokolliert die Software für den Benutzer unsichtbar Datenübertragungen jeder Art. Die mitgeschnittenen Informationen werden wahlweise auf dem Endgerät gespeichert oder direkt an den Angreifer weitergeleitet (z. B. per SMS oder E-Mail). Auch das Mitschneiden von Gesprächen oder das Mithören in Echtzeit – etwa als VoIP-Übertragung – ist möglich.

Schutzmaßnahmen siehe M.92, M.94, M.95

16.3.2 Mögliche Schutzmaßnahmen

M.92 Virenschutzprogramme

Der Einsatz von speziell auf mobile Endgeräte zugeschnittener Virenschutzprogramme schützt wirksam vor dem Befall durch Viren und anderer Schadprogramme.

M.93 Vertrauenswürdige Absender

Der Nutzer sollte nur MMS von als absolut vertrauenswürdigen Absendern speichern. Zusätzlich muss die Vertrauenswürdigkeit des Dienstanbieters gewährleistet sein, da einem Innentäter prinzipiell die Übermittlung von Schadprogrammen möglich ist.

M.94 Sicherheits-Updates

Die durch den Hersteller zur Verfügung gestellten Betriebssystem-Updates, die eventuell von Schadprogrammen genutzte Sicherheitslücken schließen, müssen zeitnah nachinstalliert werden.

M.95 Zugriffskontrolle Endgeräte

Ein unbefugter Zugriff auf das Endgerät zur Installation von (kommerzieller) Überwachungssoftware ist unbedingt zu verhindern. Daher sind besonders die allgemeinen Maßnahmen bezüglich PIN und Endgerätezugriff aus Kapitel 14.2 dieses Dokuments zu beachten.

17. Fazit

Der immense Zuwachs neuer Kommunikationsdienste, Übertragungsverfahren, Datenübertragungsraten und anderer Technologien im Bereich öffentlicher Mobilfunknetze hat dazu beigetragen, dass die Sicherheitsrisiken und Probleme in diesem Umfeld umfangreicher und erheblich komplexer geworden sind. Das Bewusstsein der Anwender ist in diesem Punkt nicht in gleichem Maße angewachsen. Die vorliegende Broschüre zeigt, dass die Nutzung öffentlicher Mobilfunksysteme auch ein Bedrohungspotenzial in sich birgt. Sowohl auf Ebene der Mobilfunknetze, als auch im Bereich von Diensten und Endgeräte-Applikationen findet sich eine Vielzahl von möglichen Angriffspunkten für Datendiebstahl und Missbrauch vertraulicher oder persönlicher Informationen.

Beispielsweise sind die im GSM-Netz genutzten Verschlüsselungsmechanismen keineswegs sicher. Viele Beispiele zeigen, wie hier einfache kriminelle Ansätze ausreichen, um Gespräche mitzuschneiden. Hinzu kommt, dass die Sicherung der Richtfunkstrecken, die in der Regel genutzt werden, um verschiedene Sendeanlagen zu verbinden, ausschließlich in der Verantwortung des Betreibers liegt. Bei UMTS sind bereits während der Standardisierung entsprechende Maßnahmen vorgesehen worden. Es wird aber noch einige Zeit vergehen, bis diese überall umgesetzt sind.

Gleichzeitig sind mit UMTS, aber auch mit GPRS und EDGE, deutlich höhere Datenübertragungsraten verbunden, die es beispielsweise zulassen, die Kamera eines mobilen Endgeräts für eine dauerhafte und qualitativ hochwertige Überwachung zu nutzen.

Doch nicht nur die Übertragungsverfahren in den mobilen Kommunikationsnetzen bergen Sicherheitslücken. Auch die im Mobilfunknetz gebotenen Dienste, wie etwa der Kurzmitteilungsdienst SMS, weisen sicherheitsrelevante Mängel auf. So unterliegen die zur Übertragung von Kurznachrichten verwendeten Steuerungskanäle (SACCH und SDCCH) zwar denVerschlüsselungsmethoden für die Luftschnittstelle des GSM-Netzes. Diese können aufgrund der einseitigen Authentifizierung nach GSM Standard jedoch leicht überwunden werden. Die in SMS versendeten Inhalte werden nicht zusätzlich verschlüsselt und bieten somit keine Ende-zu-Ende Sicherheit. Sie mitzulesen stellt für einen potenziellen Angreifer kein Problem dar. Des Weiteren können SMS missbraucht werden, um das mobile Endgerät inaktiv zu setzen (SMS-Bombe) oder Konfigurationsdaten zu manipulieren.

Durch die zunehmende Nutzung von mobilen Datendiensten und den vermehrten Zugriff auf Inhalte des Internets vom mobilen Endgerät aus erhöht sich auch die Bedrohung durch Viren, Würmer und andere Schadprogramme. Die mobilen Endgeräte, längst ähnlich leistungsfähig wie Personal Computer, werden zunehmend mit PC-ähnlichen Betriebssystemen ausgestattet, sodass die Verbreitung solcher Schadprogramme begünstigt wird. Die Folgen für den Nutzer solcher Endgeräte können vielfältig sein und reichen von erhöhten Verbindungskosten bis hin zum Verlust vertraulicher Daten.

Zur Gefährdung vertraulicher Daten kommt eine Gefährdung der Privatsphäre hinzu. Hier stellt insbesondere die Möglichkeit der Lokalisierung eine Bedrohung dar. Eine Lokalisierung wird dadurch möglich, dass die Netzbetreiber zur technischen Realisierung von Roaming und Handover auf Mechanismen zur Ortsbestimmung mobiler Teilnehmer angewiesen sind. Während solche Informationen bisher nicht gespeichert wurden und einem eventuellen Innentäter nur zum Verbindungszeitpunkt zur Verfügung standen, werden diese Daten durch die gesetz-

liche Neuregelung zur Vorratsdatenspeicherung seit Anfang des Jahres 2008 mit den Verbindungsdaten verknüpft und für einen Zeitraum von mindestens sechs Monaten auf Seiten des Providers vorgehalten. Von den Lokalisierungsmechanismen der Mobilfunknetze machen auch Ortungsdienste Gebrauch. Diese können Mobilfunkteilnehmer nach vorangegangener Anmeldung orten und diese Lokalisierungsdaten ihrem Kunden zur Verfügung stellen. Die Gefahr liegt hier in der Erschleichung des Einverständnisses des Mobilfunkteilnehmers durch Dritte. So gewonnene Lokalisierungsdaten können vielfältig missbraucht werden. Das Spektrum reicht von Marktforschungszwecken bis hin zur gezielten Überwachung von Personen.

Mit der zunehmenden Nutzung von mobilen Endgeräten im Alltag hat auch die Zahl kommerzieller Angebote für Mobilfunkkunden zugenommen. Insbesondere Handels- und Zahlungsplattformen erleben – wie auch die korrespondierenden Internetangebote – einen Zuwachs. Auch wenn die Vertraulichkeit von Finanztransaktionen im ureigensten Interesse der Dienstbetreiber liegt, bieten diese Dienste oft eine Angriffsfläche für Datendiebstahl und Manipulation. Neben dem Missbrauch entwendeter Zugangsdaten für den Zugriff auf Kundenkonten oder Guthaben besteht wiederum die Gefahr des Missbrauchs zu Marktforschungszwecken.

Doch nicht nur technische Aspekte, sondern auch das Verhalten der Nutzer von mobilen Endgeräten impliziert nicht selten Sicherheitsprobleme. Beispielsweise gehen Endgeräte mindestens zeitweise verloren. Wenn dann ein Nutzer keine Passwörter nutzt oder zentrale Möglichkeiten zum Löschen der Inhalte bestehen, hat der Finder alle Zugriffsmöglichkeiten. In diesem Punkt bieten viele Softwarehersteller bisher nur wenig überzeugende Lösungen. Zudem ist vielen Nutzern gar nicht bewusst, dass mit dem ständigen Zugriff auf Mails unter Umständen auch neue Sicherheitslücken im Bereich der firmeneigenen Festnetze entstehen. Mit herkömmlichen Firewall-Lösungen kann diese Gefährdung kaum entschärft werden.

Zwar wurden mit der Weiterentwicklung der Mobilfunktechnologie – von den ersten Anfängen hin zum heute verbreiteten UMTS – auch die Sicherheitsmechanismen der Netze verbessert. Dem gegenüber steht aber eine Diversifizierung der nutzbaren Dienste. Diese – für den Anwender fast unüberschaubare – Fülle von Leistungsmerkmalen und Diensten erhöht implizit die Zahl der Sicherheitslücken. Man könnte in diesem Zusammenhang von „insecurity through obscurity“ sprechen – der Angreifer weiß um die Schwachstellen eines Dienstes, während dem Anwender das Missbrauchspotenzial meist verborgen bleibt.

Im Bereich der Netze und Dienste sind dem Anwender häufig die Hände gebunden, insbesondere wenn es um Sicherheitsfragen geht. Oft ist die einzige gangbare Methode zur Vermeidung von Risiken der Verzicht auf die Dienstnutzung. Hier ist ein erhöhtes Engagement der Netzbetreiber und Dienstanbieter erforderlich, die – schon im Eigeninteresse – den Sicherheitsaspekten ihrer Netze besondere Aufmerksamkeit schenken sollten.

Auch die rasante Weiterentwicklung der mobilen Endgeräte zu vollwertigen, tragbaren Computern mit einer zunehmenden Monokultur der Betriebssysteme erhöht das Nutzungsrisiko. Bereits heute kämpft man mit bislang nur aus dem PC-Bereich bekannten Sicherheitsproblemen wie der Verbreitung von Viren, Würmern und Trojanischen Pferden. Diese Entwicklung wird anhalten, so dass hier ein Umdenken der Anwender gefordert ist. Das mobile Endgerät ist keineswegs eine Insel der Datensicherheit und Privatsphäre – und dennoch für viele Anwender das am häufigsten genutzte Kommunikationsmittel. Daher sollte diesem Endgerät auch in Sicherheitsfragen besonderes Augenmerk geschenkt werden, wie dies für viele Anwender beim heimischen PC schon lange selbstverständlich ist.

Die Konsequenz muss also eine erhöhte Wachsamkeit und eine etwas kritischere Haltung bei der Nutzung mobiler Kommunikationsmedien sein. Neben dem Engagement der Provider gilt dies besonders für Unternehmen und Behörden. Die Ausweitung unternehmensweiter Sicherheitskonzepte auf mobile Kommunikationswege liegt – gerade in Bereichen mit erhöhtem Schutzbedarf – im ureigensten Interesse der Unternehmen. Der wirksamste Schutz ist aber der aufgeklärte Anwender. Nur der verantwortliche und wachsame Umgang mit dem Mobilfunk und die Kenntnis um seine Risiken können nachhaltig vor dem Missbrauch persönlicher und vertraulicher Daten schützen.

18. Abkürzungen

Ziffern

16QAM	sechzehnfache Quadratur Amplituden Modulation
3DES	Triple DES (auch TDES abgekürzt)
3G	dritte Generation mobiler Kommunikationssysteme
3GPP	3rd Generation Partnership Project
4-PSK	vierfaches Phase Key Shifting
4G	4th Generation Network
8-PSK	achtfaches Phase Key Shifting

A

AGB	Allgemeine Geschäfts-Bedingungen
AK	Authentication Key
AKA	Authentication and Key Agreement
AMF	Authenticated Management Field 16 Bit
AMR	Adaptive Multirate Codec
AMR-W	Adaptive Multirate Wideband Codec
ATM	Asynchronous Transfer Mode
AuC	Authentication Center
AUTN	Authentication Token
AV	Authentication Vector

B

BCCH	Broadcast Control Channel
BDSG	Bundesdatenschutzgesetz
BGAN	Broadband Global Area Network
Bit	Binary Digit
BOS	Behörden und Organisationen mit Sicherheitsaufgaben
BPSK	Binary Phase Shift Keying
BSC	Base Station Controller
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSS	Base Station Subsystem
BTS	Base Transceiver Station

C

CBC	Cipher Block Chaining

CI	Cell Identifier
CID	Cell ID
CIM D2	Computer Interface to Message Distribution Version 2 (Nokia)
CK	Ciphering Key 128 Bit für die Verschlüsselung (bei GSM Kc 64 Bit)
CN	Core Network
CRM	Customer Relationship Management
CS	Coding Scheme
CSD	Circuit Switched Data
COPUOS	COmmittee on the Peaceful Use of Outer Space

D

DECT	Digital Enhanced Cordless Telecommunication
DES	Data Encryption Standard
DoS	Denial of Service
DM	Device Management
DNS	Domain Name System
DS	Data Synchronisation

E

E-Commerce	Electronic Commerce
E-Payment	Electronic Payment
ECSD	HSCSD mit EDGE
EDGE	Enhanced Data Rates for GSM Evolution
EDR	Enhanced Data Rate
EGPRS	GPRS mit EDGE
EGSM	Extended GSM
EIR	Equipment Identity Register
E-Mail	Electronic Mail
EMI-UCP	Extended Machine Interface-Universal Computer Protocol
EMS	Enhanced Messaging Service
EMSI	Encrypted Mobile Subscriber Identity
ETSI	European Telecommunication Standards Institute

F

FCB	Frequency Correction Burst
FDD	Frequency Division Duplex
FDM	Frequency Division Multiplexing

FDMA	Frequency Division Multiple Access
FOTA	Firmware Over The Air

G

GEA	GPRS Encryption Algorithm
GERAN	GSM EDGE Radio Access Network
GEO	Geostationary Earth Orbiting
GGSN	Gateway GPRS Support Node
GMSC	Gateway Mobile Switching Center
GMSK	Gaussian Minimum Shift Keying
GPRS	General Packet Radio Service - Paketvermittelter Datendienst auf Basis von GSM
GPS	Global Positioning System
GSM	Global System for Mobile Communications (ehem. Groupe Spéciale Mobile)
GTP	GPRS Tunnelling Protocol

H

HLR	Home Location Register
HSCSD	High Speed Circuit Switched Data
HSDPA	High Speed Downlink Packet Access
HSOPA	High Speed OFDM Packet Access
HSUPA	High Speed Uplink Packet Access
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure

I

ID	Identification Number
IDEA	International Data Encryption Algorithm
IK	Integrity Key für die Datenintegrität (12 Bit)
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IrDA	Infrared Data Association (Infrarot-Schnittstelle)
ISDN	Integrated Services Digital Network (ehem. Integriertes Sprach- und Datennetz)
ISM	Industrial-Science-Medical
ISO	International Organisation for Standardization

IT	Information Technology
ITU	International Telecommunication Union

L

LA	Location Area
LAN	Local Area Network
LAI	Location Area Identity
LAC	Local Area Code
LBS	Location Based Services
LEO	Low Earth Orbiting
LLC	Logical Link Control
LTE	Long Term Evolution

M

M-Commerce	Mobile-Commerce
M-Payment	Mobile Payment
MABEZ	Massenverkehr zu bestimmten Zielen
MAC	1. Media Access Control
	2, Message Authentication Code
MCC	Mobile Country Code
ME	Mobile Equipment
MMC	Multimedia Card (digitales Speichermedium)
MMS	Multimedia Messaging Service
MMSC	Multimedia Message Service Center
MNC	Mobile Network Code
MNO	Mobile Network Operator
MPDS	Mobile Packet Data Service
MS	Mobile Station
MSC	Mobile Switching Center
MSISDN	Mobile Station ISDN Number
MSK	Minimum Shift Keying
MSS PP	Mobile Synchronisation Services Protection Profile
MVNE	Mobile Virtual Network Enabler
MVNO	Mobile Virtual Network Operator

N

NAT	Network Address Translation

NFC	Near Field Communication
NGMN	Next Generation Mobile Network
NGN	Next Generation Network
NMC	Network Management Center
NOC	Network Operation Center
Node-B	Funkzelle in UMTS Nomenklatur (entspricht BTS in GSM-Netz)
NRZ	Non Return Zero
NSS	Network Subsystem

O

ÖPNV	Öffentlicher Personennahverkehr
OFDM	Orthogonal Frequency Division Multiplexing
OMA	Open Mobile Alliance
OMC	Operations and Maintenance Center
OSI	Open System Interconnection
OSS	Operations and Support System
OTA	Over the Air
OTAP	OTA Provisioning
OTASP	OTA Service Provisioning

P

PAP	Push Access Protocol
PGSM	Primary GSM
PIM	Personal Information Management
PIN	Personal Identification Number
PoC	PTT over Cellular
PPG	Push Proxy Gateway
PUK	Personal Unblocking Key
PSTN	Public Switched Telephone Network
PTT	Push-To-Talk

Q

QPSK	Quadrature Phase Key Shifting (4-PSK)

R

RAND	eine nicht vorhersagbare Zufallszahl
RBGAN	Regional BGAN
RC5	Rivest Cipher 5

RFID	Radio Frequency Identification
RLC	Radio Link Control
rMVNO	roaming Mobile Virtual Network Operator
RNC	Radio Network Controller
RNS	Radio Network Subsystem
RTCP	Real Time Control Protocol
RTP	Real Time Protocol

S

SAT	SIM Application Toolkit
SGSN	Service GPRS Support Node
SD	Secure Digital
SI	Service Indication
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SL	Service Load
SMIL	Synchronised Multimedia Integration Language
SMPP	Short Message Peer to Peer
SMS	Short Message Service
SMS-MO	SMS Mobile Originated
SMS-MT	SMS Mobile Terminated
SMSC	SMS Center
SNR	Signal Noise Ration
SQN	Sequenznummer
SQN+AK	verschleierte 48 Bit Sequenznummer (SQN) mittels XOR Verknüpfung mit dem 48 Bit Anonymity Key (AK)
SRTP	Secure RTP
SS7	Signalling System No.7
SSL/TLS	Secure Socket Layer/Transport Layer Security

T

TA	Timing Advance
TAN	Transaktionsnummer
TAP	Telecator Alphanumeric Protocol (Motorola)
TBCP	Talk Burst Control Protocol
TCP	Transport Control Protocol
TDD	Time Division Duplex

TDDSG	Teledienstschutzgesetz
TDG	Teledienstgesetz
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TDSV	Telekommunikationsdatenschutzverordnung
TE	Terminal
TEMSI	Temporary Encrypted Mobile Subscriber Identity
TETRA	Terrestrial Trunked Radio
TKG	Telekommunikationsgesetz
TKÜV	Telekommunikationsüberwachungsverordnung
TLS	Transport Layer Security
TMSI	Temporary Mobile Subscriber Identity
TOE	Target of Evaluation

U

UA	User Agent
UAProf	User Agent Profile
UE	User Equipment
UDP	User Datagram Protocol
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunication System
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USIM	Universal Subscriber Identity Module
USSD	Unstructured Supplementary Service Data
UTRAN	UMTS Terrestrial Radio Access Network

V

VASP	Value Added Services Provider
VLR	Visitor Location Register
VoIP	Voice over IP
VPN	Virtual Private Network

W

W-CDMA	Wideband Code Division Multiple Access
WAE	Wireless Application Environment
WAP	Wireless Application Protocol

WDP	Wireless Datagram Protocol
WIM	WAP Identity Module
WLAN	Wireless Local Area Network
WSP	Wireless Session Protocol
WTA	Wireless Telephony Application
WTAI	Wireless Telephony Application Interface
WTLS	Wireless Transport Layer Security
WTP	Wireless Transaction Protocol

X

XEMSI	Extended Encrypted Mobile Subscriber Identity
XHTML	Extensible Hypertext Markup Language
XMAC	Expected Message Authentication Code
XML	Extensible Markup Language
XRES	Expected Response zur Teilnehmer-Authentifizierung (bei GSM SRES 32 Bit)

19. Literatur / Links

Die Funktionalität und Aktualität der angegebenen Links wurde am 3. Juni 2008 überprüft.

[3GPP] The 3rd Generation Partnership Project, http://www.3gpp.org

[3GPP21133] The 3rd Generation Partnership Project, Technical Specification 21.133, 3G Security; Security threats and requirements, http://www.3gpp.org/ftp/Specs/html-info/21133.htm, 07. Januar 2002

[3GPP22038] The 3rd Generation Partnership Project, Technical Specification 22.038, http://www.3gpp.org/ftp/Specs/html-info/22038-CRs.htm, 07. März 2007

[3GPP23140] The 3rd Generation Partnership Project, Technical Specification 23.140, Multimedia Messaging Service (MMS); Functional description ; Stage 2, http://www.3gpp.org/ftp/Specs/html-info/23140.htm, 25. März 2008

[3GPP26140] The 3rd Generation Partnership Project, Technical Specification 26.140, Multimedia Messaging Service (MMS); Media formats and codes http://www.3gpp.org/ftp/Specs/html-info/26140.htm, 21. Juni 2007

[3GPP33107] The 3rd Generation Partnership Project, Technical Specification 33.107, 3G security; Lawful interception architecture and functions, http://www.3gpp.org/ftp/Specs/html-info/33107.htm, 20. März 2008

[BiDu33401] Eli Biham and Orr Dunkelman, "Cryptanalysis of the A5/1 {GSM} Stream Cipher", 2000, http://citeseer.ist.psu.edu/701770.html

[BMJ07] Pressemitteilung des Bundesministerium der Justiz, http://www.bmj.bund.de/enid/590601920cf71891a0cf2593af66c730,46bdaa706d635f6964092d0934383133093a095f7472636964092d0933303334/Pressestelle/Pressemitteilungen_58.html, 09. November 2007

[BSIDlKSa] Bundesamt für Sicherheit in der Informationstechnik, Local Wireless Communication, Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte, 2003, http://www.bsi.de/literat/doc/drahtloskom/drahtloskom.pdf

[BSIEiI] Bundesamt für Sicherheit in der Informationstechnik, Einkaufen im Internet, http://www.bsi-fuer-buerger.de/einkaufen/

[BSIfB] Bundesamt für Sicherheit in der Informationstechnik, BSI für Bürger, http://www.bsi-fuer-buerger.de/

[BSIMDS] Mobilfunkdetektor MDS des Bundesamt für Sicherheit in der Informationstechnik, http://www.bsi.de/produkte/mds/index.htm

[BSIMoEMoA] Bundesamt für Sicherheit in der Informationstechnik, Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen, 2006, http://www.bsi.bund.de/literat/doc/mobile/mobile_endgeraete.pdf

[BSIMSSPP] Bundesamt für Sicherheit in der Informationstechnik, Common Criteria Protection Profile, Mobile Synchronisation Services (MSS PP), BSI-PP-0034-2007, http://www.bsi.bund.de/zertifiz/zert/reporte/PP0034b.pdf

[BSIOB] Bundesamt für Sicherheit in der Informationstechnik, Online Banking, http://www.bsi-fuer-buerger.de/geld/

[BSIPh] Bundesamt für Sicherheit in der Informationstechnik, Phishing – gefährliche Umleitung für Ihre Passwörter, http://www.bsi-fuer-buerger.de/phishing/

[BSIRFID] Bundesamt für Sicherheit in der Informationstechnik, Risiken und Chancen des Einsatzes von RFID-Systemen, 2004, http://www.bsi.de/fachthem/rfid/RIKCHA.pdf

[DBTtkue] Deutscher Bundestag Drucksache 16/5846, 27. Juni 2007, "Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG" - http://dip.bundestag.de/btd/16/058/1605846.pdf

[DSBer20] Datenschutz Berlin, Berliner Datenschutzbeauftragter, “Mobilfunk und Datenschutz”, 1994, http://www.datenschutz-berlin.de/attachments/51/Materialien20.pdf?1166527210

[DuD26002] Dirk Fox, Datenschutz und Datensicherheit, “Der IMSI-Catcher”, 2002 http://www.datenschutz-und-datensicherheit.de/jhrg26/imsicatcher-fox-2002.pdf

[ECMA262] ECMA, Standardizing Information and Communication Systems, Standard ECMA-262, 3rd Edition, Dezember 1999, http://www.ecma-international.org/publications/files/ECMA-ST/Ecma-262.pdf

[ETS300] European Telecommunication Standards Institute, 1992-07 DE/PS-03001-3 Title: Paging Systems (PS); Source: PS 3 European Radio Message System (ERMES) Part 3: Network aspects 296 Pages ETSI Price Code: T Scope: ERMES System Architecture Numbering, Addressing and Identification Call Processing Interfaces 12, 13, 14, 15 and 16 PNC Specification. PAC Specification

[FWA08] Der Fischer Weltalmanach, Griechenland – Abhörskandal, Webseite der Bundeszentrale für politische Bildung, http://www.bpb.de/wissen/VWWV1X,4,0,Griechenland.html

[GLST] Webauftritt von Globalstar, http://www.globalstar.com

[GSKBSI] Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kataloge, Stand 9. Ergänzungslieferung, http://www.bsi.bund.de/gshb/deutsch/index.htm

[HeBuTi40] Prof. Dr. Cornelius Herstatt, Dr. Stephan Buse, Dipl.-Kfm. Rajnish Tiwari: The mobile commerce technologies: generations, standards and protocols, Juli 2006, http://www1.uni-hamburg.de/m-commerce/articles/Working_Paper_40.pdf

[INMS] Webauftritt der Inmarsat plc, http://www.inmarsat.com

[IRID] Webauftritt der Iridium Satellite LLC, http://www.iridium.com

[MeWe04] Meyer, U. and Wetzel, S. 2004. A man-in-the-middle attack on UMTS. In Proceedings of the 3rd ACM Workshop on Wireless Security (Philadelphia, PA, USA, October 01 - 01, 2004). WiSe '04. ACM, New York, NY, 90-97. DOI= http://doi.acm.org/10.1145/1023646.1023662

[NGMN06] White Paper "Next Generation Mobile Networks Beyond HSPA & EVDO" by Board Of NGMN Limited, 5. Dezember 2006, Version 3.0, http://www.ngmn.org/fileadmin/content/documents/downloads/White_Paper_-_Beyond_HSPA_and_EVDO.pdf

[OMAcont] Open Mobile Alliance, Firmware Update Management Object, V.1.0.1, http://www.openmobilealliance.org/Technical/release_program/docs/copyrightclick.aspx?pck=FUMO&file=V1_0_1-20080331-A/OMA-TS-DM-FUMO-V1_0-20070209-A.pdf , veröffentlicht am 09. Februar 2007

[OMAsync] Open Mobile Alliance, SyncML Sync Protocol, Version 1.0.1, 15. Juni 2001, http://www.openmobilealliance.org/tech/affiliates/LicenseAgreement.asp?DocName=/syncml/spec1-0-1.zip

[OMAWWP] Open Mobile Alliance – WAP White Paper, Juni 2000, http://www.wapforum.org/what/WAP_white_pages.pdf,

[PrPo50781] http://www.presseportal.de/pm/50781/254019/2way_interactive_gmbh, 01. Juni 2001

[RFC2246] The Internet Society, Network Working Group, RFC 2246, The TLS Protocol, Version 1.0, 1999, http://www.rfc.net/rfc2246.html

[RFC2617] The Internet Society, Network Working Group, RFC 2617, HTTP Authentication: Basic and Digest Access Authentication, 1999, http://www.rfc.net/rfc2617.html

[RFC2817] The Internet Society, Network Working Group, RFC 2817, Upgrading to TLS Within HTTP/1.1, 2000, http://www.rfc.net/rfc2817.html

[Rue07] Christiane Rütten, GSM Sicherheit: Lauschgelegenheit, c't 24/2007, S90, http://www.heise.de/ct/07/24/090/

[SMIL] W3C, Synchronized Multimedia Integration Language, 15. Januar 2008, http://www.w3.org/TR/SMIL3/

[THUR] Webauftritt von Thuraya, http://www.thuraya.com/

[WAP192] Wireless Application Protocol Forum, WAP-192-WBXML-20010725-a, Version 1.3, 25. Juli 2001, http://www.openmobilealliance.org/tech/affiliates/wap/wap-192-wbxml-20010725-a.pdf

[WAP205] Wireless Application Protocol Forum, WAP MMS Architecture Overview, WAP-205-MMSArchOverview-20010425-a, 25. April 2001, http://www.openmobilealliance.org/tech/affiliates/wap/wap-205-mmsarchoverview-20010425-a.pdf

[WAP209] Wireless Application Protocol Forum, MMS Encapsulation Protocol, WAP-209-MMSEncapsulation-20020105-a, 05. Januar 2002, http://www.openmobilealliance.org/tech/affiliates/wap/wap-209-mmsencapsulation-20020105-a.pdf

[WAP210] Wireless Application Protocol Forum, WAP Architecture, WAP-210-WAPArch-20010712, 12. Juli 2001, http://www.openmobilealliance.org/tech/affiliates/wap/wap-210-waparch-20010712-a.pdf

[WAP224] Wireless Application Protocol Forum, Wireless Transaction Protocol, WAP-224-WTP-20010710-a, 10. Juli 2001, http://www.openmobilealliance.org/tech/affiliates/wap/wap-224-wtp-20010710-a.pdf

[WAP230] Wireless Application Protocol Forum, Wireless Session Protocol Specification, WAP-230-WSP, 05. Juli 2001, http://www.openmobilealliance.org/tech/affiliates/wap/wap-230-wsp-20010705-a.pdf

[WAP236] Wireless Application Protocol Forum, Wireless Application Environment Specification, Version 2.0, WAP-236-WAESpec-20020207-a, 07. Februar 2002, http://www.openmobilealliance.org/tech/affiliates/wap/wap-236-waespec-20020207-a.pdf

[WAP238] Wireless Application Protocol Forum, WAP-238-WML-20010911-a, 11. September 2001, http://www.openmobilealliance.org/tech/affiliates/wap/wap-238-wml-20010911-a.pdf

[WAP259] Wireless Application Protocol Forum, Wireless Datagram Protocol, WAP-259-WDP-20010614-a, 14. Juni 2001, http://www.openmobilealliance.org/tech/affiliates/wap/wap-259-wdp-20010614-a.pdf

[WAP260] Wireless Application Protocol Forum, Wireless Identity Module, Part: Security, WAP-260-WIM-20010712-a, 12. Juli 2001, http://www.openmobilealliance.org/tech/affiliates/wap/wap-260-wim-20010712-a.pdf

[WAP261] Wireless Application Protocol Forum, Specification Information Note, WAP-261-WTLS-20010406-a, 27. Oktober 2001,

http://www.openmobilealliance.org/tech/affiliates/wap/wap-261_102-wtls-20011027-a.pdf

[WAP266] Wireless Application Protocol Forum, WAP Wireless Telephony Application, WAP-266-WTA-20010908-a, 08. September 2001, http://www.openmobilealliance.org/tech/affiliates/wap/wap-266-wta-20010908-a.pdf

[WAP268] Wireless Application Protocol Forum, WAP Wireless Telephony Application Interface, WAP-268-WTAI-20010908-a, 08. September 2001, http://www.openmobilealliance.org/tech/affiliates/wap/wap-268-wtai-20010908-a.pdf