Einführung in

Global System for Mobile Communication (GSM)

Stefan Eglauf
Samuel Frempong

Autoren

Stefan Eglauf	Bändlistr.61	8064 Zürich	seglauf@hsr.ch
Samule Frempong	Bettstenstr.2	8305 Dietlikon	sfrempon@hsr.ch

Betreuer

Dr. P. Heinzmann	cnlab AG	8640 Rapperswil	peter.heinzmann@cnlab.ch
Max Wegmüller	CN Labor	8640 Rapperswil	max.wegmueller@hsr.ch

Inhaltsverzeichnis

1.0 Einführung

1.1 Die GSM-Systemarchitektur

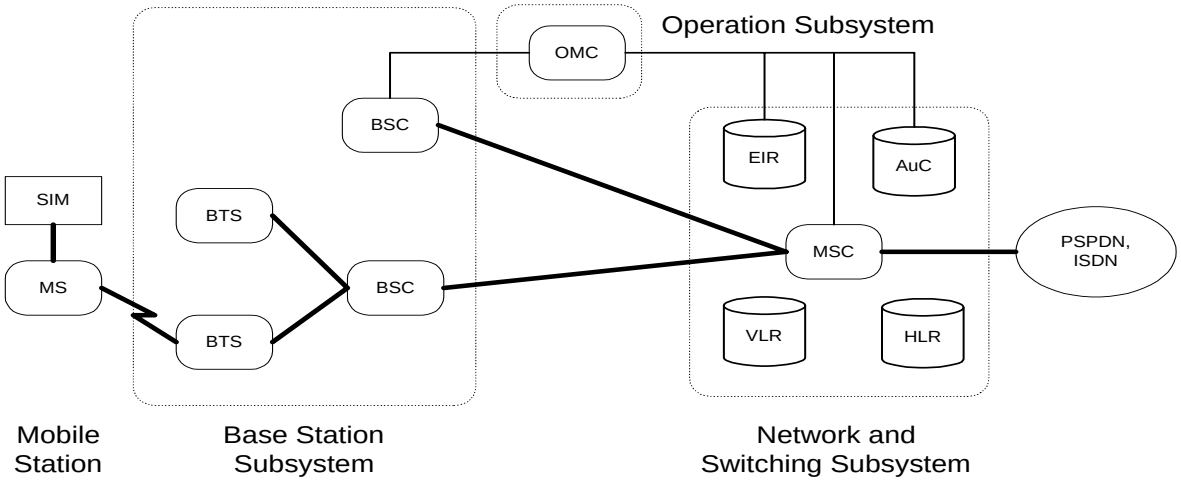


ABBILDUNG 1. GSM-Systemarchitektur

Das GSM-Netz lässt sich am besten als hierarchisch gegliedertes System verschiedener Netzelemente verstehen. Am unteren Ende steht die Mobile Station (MS), die über Funk mit der nächstgelegenen Base Tranceiver Station (BTS) kommuniziert. Zur Lenkung und Kontrolle der BTS werden sie gebietsweise von einem Base Station Controller (BSC) zusammengefasst. Das den BSC wiederum übergeordnete Netzelement, sind die Mobile Switching Centers (MSC), sie sind unter anderem für den Übergang in andere (in- oder ausländische) Telefonnetze verantwortlich.

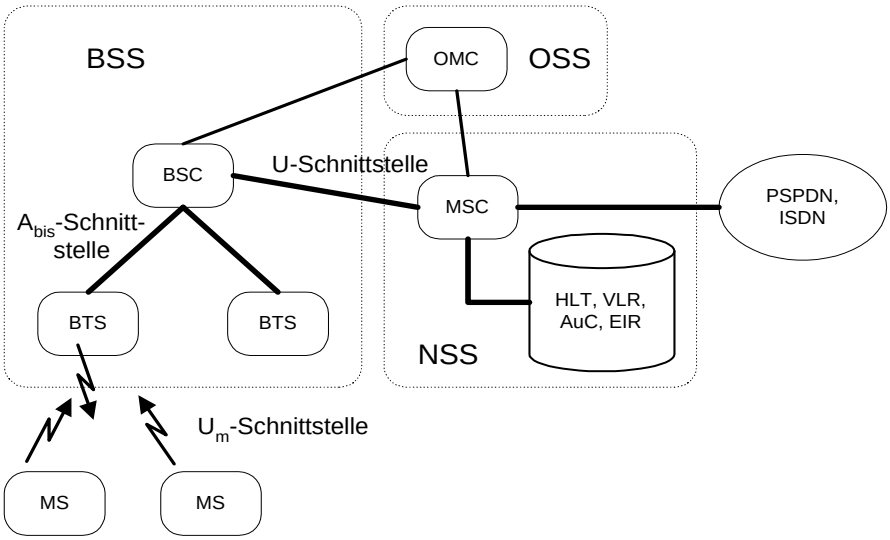


ABBILDUNG 2. Schnittstellen

Wie in Abbildung 2 ersichtlich, trägt jede Schnittstelle zwischen den einzelnen Netzelementtypen einen eigenen Namen:

- Die Um-Schnittstelle oder Funkschnittstelle (Radio-Path) zwischen Ms und BTS
- Die Abis-Schnittstelle für die Kommunikation zwischen BTS und BSC
- Die A-Schnittstelle zwischen BSC und MSC

Die genaue physikalische Ausprägung der beiden letztgenannten Verbindungen ist von untergeordneter Bedeutung. Je nach Standort kann dies per Richtfunk, über öffentliche Mietleitungen oder direkte Kabelanbindung erfolgen.

Betrachten wir nun das ganze System aus dem Blickwinkel der logischen Aufgabenverteilung, so ergibt sich eine Dreiteilung:

- Base Station Subsystem (BSS)
  Das BSS beinhaltet den eigentlichen “Funktechnik”-Teil des Systems.
- Network and Switching Subsystem (NSS)
  Wie der Name schon sagt, ist hiermit die Vermittlungstechnik gemeint. Das NSS umfasst damit die Netzelemente und Technik ab (und zwischen) der/den MSC. Wie in Abbildung 1 gezeigt, sind der MSC mehrere Datenbanken zugeordnet (HLR,VLR, AuC, EIR).
- Operation Subsystem (OSS)
  Dieses Betriebs- und Wartungssystem wird hierarchisch neben die schon erwähnten Netzelemente gestellt. Dies ist verständlich, da die verschiedenen Netzelemente überwacht werden müssen. Die Überwachungsmassnahmen selber werden durch das Operation and Maintenance Center (OMC) ferngesteuert. OMC’s werden typischerweise bei den MSC‘s angesiedelt.

Um die anfallenden Vermittlungs- und Verwaltungsaufgaben bewältigen zu können, wird eine Reihe von Datenbanken benötigt. Diese sind meist auf der MSC-Ebene angesiedelt.

Dies sind:

- Home Location Register (HLR)
  Hier werden die persönlichen Informationen des Benutzers wie Telefonnummer, freigeschaltete Dienste und so weiter gespeichert. Pro GSM-Netz gibt es nur ein HLR.
- Visitor Location Register (VLR)
  Das VLR enthält die dynamischen Teilnehmerdaten. Es handelt sich um lokale, einem Gebiet zugeordnete Datenbanken, welche Kopien der HLR-Datenbestände für die Benutzer führen, die sich momentan in ihrem Zuständigkeitsbereich befinden.
- Authentication Center (AuC)
  Das AuC enthält die Zugangsdaten der einzelnen Benutzer, insbesondere der persönlichen, geheimen SIM-Karten-Schlüssel, die zum Zugang ins Mobilfunknetz und anschliessend für die codierte Übertragung der Gesprächsdaten über das Netz notwendig sind.
- Equipment Identity Register (EIR)
  Im EIR werden die MS spezifischen Daten, insbesondere eine Liste der IMEI-Nummern, geführt.

1.2 Geschichte der Funktechnik

Bereits 1873 wies der schottische Mathematiker Maxwell die Existenz elektromagnetischer Wellen experimentell nach. Den Beweis dieser These durfte er aber nicht mehr erleben. 1895 versuchte ein 21 Jahre junger Forscher Namens Guglielmo Marchese Marconi Informationen drahtlos zu übertragen. Dazu baute er eine Apparatur auf, mit der er mittels eines Funkeninduktors hochfrequente Spannungen auf eine Drahtantenne leitete. Als Empfänger diente eine Antenne, in die ein Fritter geschalten war (ein kleines, mit Metallspänen gefülltes Vakuumglasröhrchen, das beim Auftreten hochfrequenter Signale leitend wird). Diese steuerte eine Klingel, die das Signal akustisch wiedergab. Schon sein Versuch funktionierte über eine Strecke von 1,6km. Die weiteren Entwicklungen von M.Marconi wurden von der britischen Post gesponsert, und schliesslich gründete der Italiener 1897 in London die “Marconi Wireless Telegraphy Company”.
Die ersten Versuche mit mobiler Telefonie gab es schon anfangs der dreissiger Jahre. Die “Mobilität” war aber an einen LKW mit der Übertragungstechnik gebunden. Das erste kommerzielle System stellte AT&T 1946 in St. Louis vor. Die Basisstation verwendete 6 fest zugewiesene FM-Kanäle.
Um die Kapazität zu erhöhen, kam man danach sehr schnell auf die Idee, die Kanäle dynamisch nach Bedarf zu vergeben und die Funkfrequenzen in der Form eines Zellrasters wiederzuverwenden (Die Bell-Laboratories erhielten bereits 1947 ein Patent auf dieses Verfahren). Die Technik war aber für einen kommerziellen Einsatz einfach noch nicht soweit.
In den 80er Jahren breiteten sich analoge Mobilfunknetz in Europa (vor allem in Skandinavien, Frankreich, Deutschland und Grossbritannien) sehr schnell aus. Jedes Land entwickelte ihr eigenes System, welches zu den Anderen nicht kompatibel war.
Um einen einheitlichen Europäischen Standard zu entwickeln, gründetet Conférance Européenne des Administrations des Postes et des Télécommunications (CEPT) 1982 eine Standardisierunsgruppe Groupe Spécial Mobile (GSM). Die Arbeit an diesem Standard dauerte bis 1987, als das GSM Memorandum of Understanding (MoU) von Repräsentanten verschiedener Telefongesellschaften aus 17 Ländern unterzeichnet wurde. 1988 wurde die Arbeit an GSM der Standardisierungsorganisation ETSI übertragen. Dadurch wurde der GSM-Standard zu einer wirklich offenen, industrieweiten Entwicklung. Im Zuge der weltweit stürmischen Verbreitung der GSM-Netze ist GSM in Global System for Mobile Communication benannt worden.
Nach dem offiziellen Start der GSM-Netze in Sommer 1992 nahm die Teilnehmerzahl rasch zu.

Überblick (Schweiz und weltweite Entwicklung)

[2], [28]

1946	In St.Louis (Missouri, USA) wird der erste Mobiltelefon-Service angeboten
1978	CEPT entscheiden sich, ein 900 MHz Band für die Mobilkommunikation in Europa zu reservieren
1978	In der Schweiz wird das erste Mobiltelefonnetz NATEL A in Betrieb genommen
1979	In Chicago (USA) wird das erste Mobiltelefonnetz der USA in Betrieb genommen (AMPS System)
1082	Infolge der grossen Nachfrage wird das Nachfolgenetz NATEL B in der Schweiz installiert
1987	Bei der Einführung des NATEL C entscheidet sich die Schweiz für das leistungsfähigere NMT-System (Nordic Mobil Telephone) im 900 MHz Band
1982 - 1990	Das ETSI entwickelt mit der europäischen Industrie den GSM-Standard
1991	An der Telecom in Genf wird das GSM-System erstmals präsentiert
1993	Die ersten Roaming-Abkommen werden geschlossen, und erste kommerzielle Dienste ausserhalb Europa angeboten
1994	Datendienste werden für das GSM-System angeboten
1995	Fax, Daten und SMS Roaming für GSM
1996	Januar 1996: 120 GSM-Netze sind in 71 Ländern in Betrieb Juni 1996: 133 GSM-Netze in 81 Länder sind in Betrieb
1998	Juli 1998: Weltweit 100 Millionen GSM Benutzer. Aktuelle Daten zu GSM findet man in http://www.gsmworld.com

TABELLE 1. Entwicklungen

AMPS: Advanced Mobile Phone Services
TACS: Total Access Communication System Derivate, von AMPS AMPS und TACS sind nicht kompatibel zu GSM
CEPT: Conférance Européenne des Administrations des Postes et des Télécommunications
ETSI: European Telecommunications Standards Institute
GSM: Global System for Mobile Communications
NATEL: Nationales Auto-TelefonWeltweite Mobiltelefon Netze

1.3 Weltweite Mobiltelefon Netze

1.3.1 Analoge Netze

[2]

Bis 1992 wurden nur Mobiltelefone mit analoger Technologie (1. Generation) benutzt. Weltweit gab es viele unterschiedliche Systeme:

[30]

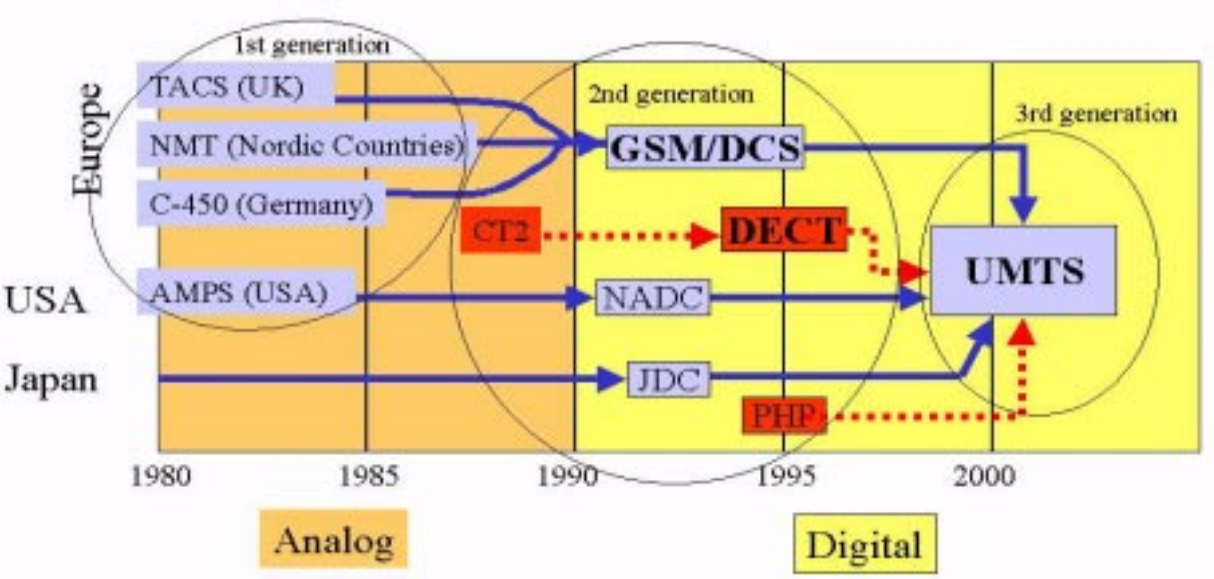


ABBILDUNG 3. Überblick der weltweiten Mobilfunknetze

[2]

Analoge Systeme	Land	Frequenzbereich
Advanced mobile phone service (AMPS)	U:S:A:	800 MHz
Total access communication system (TACS)	U.K.	900 MHz
Nordic Mobile telephone system (NMT)	Skandinavien, Schweiz, Spanien	450+950 MHz
C-Netz	Deutschland, Portugal, Südafrika	450 MHz
Radiocom 2000	Frankreich	
RTMI/RTMS	Italien	

TABELLE 2. Analoge Netze

Da es eine Vielzahl von verschiedenen analogen Mobiltelefonnetzen gab, die in verschiedenen Frequenzbändern arbeiteten und unterschiedliche Signale und Protokolle benutzten, war es unmöglich, nur ein Telefon in ganz Europa zu benutzen. Nach den analogen Systemen folgten die digitalen Systeme, und man wollte einen einheitlichen europäischen Standard entwickeln.

1.3.2 Weshalb ein digitales Netz ?

[2]

- Da die Anzahl neuer Abonnenten ständig wuchs, hatte man vor allem in den Städten ein Kapazitätsproblem. Durch digitale Zeitmultiplexierung dachte man, dieses Problem lösen zu können.
- Bei der analogen Übertragung wird die Tonqualität durch die Funkübertragung beeinflusst. Fehler die auf der Übertragungsstrecke entstehen, z.B. Interferenzen, werden als Störsignale wahrgenommen. Bei der digitalen Übertragung kann mittels Codierung und Fehlerkorrektur das ankommende Signal rekonstruiert werden, solange die Störungen ein gewisses Mass nicht überschreiten.

1.3.3 Digitale Netze

Überblick der Amerikanischen Systeme

Das Ziel war es, die Kapazität des existierenden AMPS Systems mit digitaler Technologie zu vergrössern. Durch Zeitmultiplexierung wurde dies erreicht. Ein Kanal wird in Zeitschlitze von 13ms unterteilt (TDMA). Da das Netz im Dual-Modus arbeitet, wird, sofern ein digitales Netz vorhanden ist, auf digital umgeschaltet und sonst analog übertragen.

EUROPA-GSM

Eigentlich war es keine Voraussetzung, dass das GSM-Netz digital sein sollte. Die Entscheidung, das Netz digital zu machen, wurde bei der Entwicklung der GSM-Standards festgelegt.

[2]

Digitale Systeme	Land	Bemerkung
Advanced mobile Phone Standard (AMPS)	U.S.A.	equivalent zu IS-54 und NADC Arbeiten im Dual-Modus *1)*
Code division multiple access (CDMA) *2)*	U.S.A.	equivalent zu IS-95 Arbeitet im Dual-Modus
Japanese digital cellular (JDC)	Japan	800 MHz + 1,5 GHz arbeitet im Dual-Modus
Personal digital cellular (PDC)	Japan	arbeitet im Dual-Modus
Global System for Mobile Communication (GSM)	Europa	

TABELLE 3. Digitale Netze

1) Dual-Modus: Sofern ein digitales Netz vorhanden ist, wird auf digital umgeschaltet und sonst analog übertragen.

2) CDMA Technologie wurde für militärische Anwendungen in den 60 Jahren entwickelt

1.3.4 Weltweite Netze und Abonnenten

http://www.gsmworld.com

Es wird geschätzt, dass es weltweit 260 Millionen Mobiltelefon-Abonnenten gibt. Ca. 100 Millionen Abonnenten benutzen GSM, was 38 % des Mobiltelefon-Marktes ausmacht. Weltweit hat das CDMA System ungefähr 12 Millionen Abonnenten, 75% Prozent dieser Abonnenten sind in Asien. Es wird vorausgesagt, dass im Jahr 2003 die Hälfte der Bevölkerung in Hong Kong und Singapore Mobiltelefone benutzen wird. Deshalb wird es entscheidend sein, welches System sich in Asien durchsetzt.

[30]

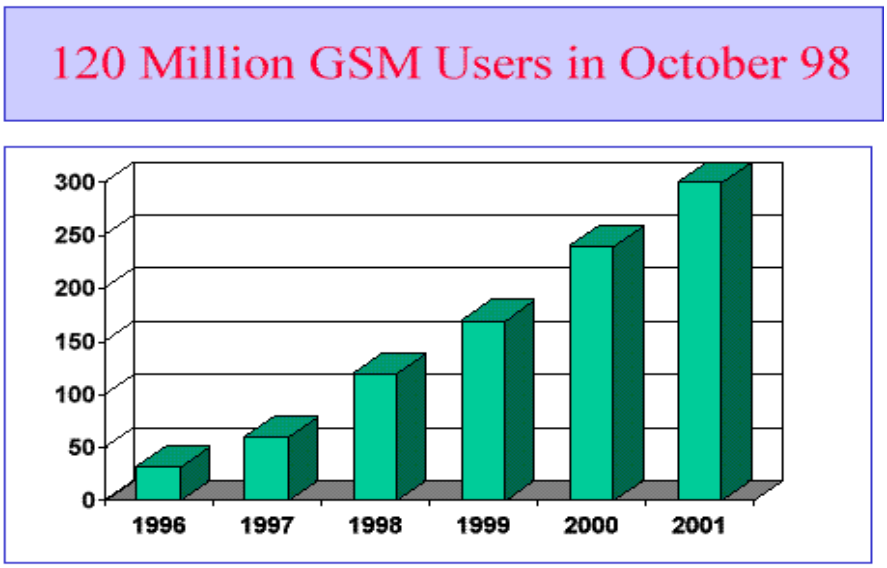


ABBILDUNG 4. GSM-Abonnenten

1.3.5 Mobilfunkwachstum

[15]

Der Markt für die private Mobilkommunikation wächst in gewaltigen Sprüngen. Führend dabei ist Skandinavien, allen anderen voran Finnland, wo nach Angaben des nationalen Kommunikationsministeriums bereits im Sommer 1998 ein Handyanteil von 50% erreicht wurde. Das Ministerium rechnet mit 60% Handydichte im Jahr 1999, was dann bedeuten wird, dass erstmals in der Geschichte des Telefons in einem Land der Erde die mobile Variante des Geräts häufiger benutzt wird als die herkömmliche.

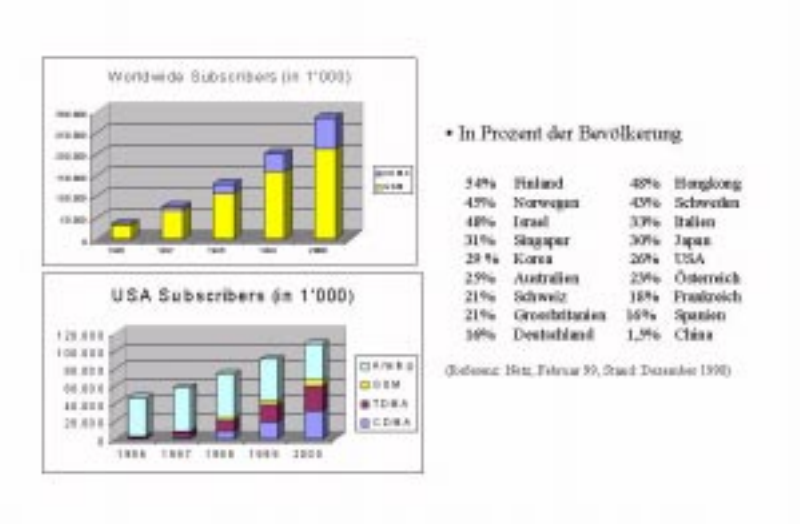


ABBILDUNG 5. Weltweite Netze und Abonnenten (Juli 1998)

Vor diesem Zahlenhintergrund ist es kaum verwunderlich, dass Fachleute mittlerweile mit der gänzlichen Ablösung der herkömmlichen Telefone durch mobile Geräte rechnen. Juha Lappalainen, Marketing- und Kundenbetreuunsgschef der GSM-Netzwerk- und Funkabteilung von Nokia Telecommunications ist überzeugt, dass Sprachkommunikation drahtlos werden wird. Die heutige mobile Technik genüge in jeder Hinsicht vollauf, um die Festnetze komplett zu ersetzen.

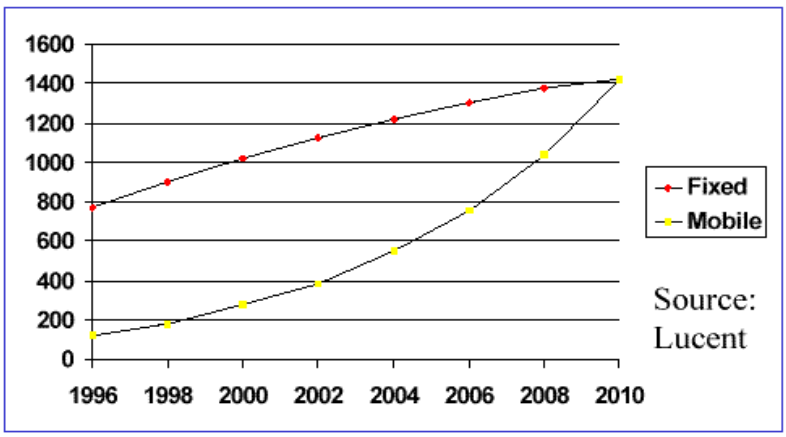


ABBILDUNG 6. Vergleich Fixe-, Mobilanschlüsse

Das Büro wird eines der nächsten Einsatzgebiete für das Handy, auch wenn die meisten der zukünftigen Grosskunden davon noch gar nichts ahnen. In einem Strategiepapier des Handy- und Netzherstellers Ericson beispielsweise sind grosse Unternehmen und Verwaltungen eindeutig als nächstes besonders wichtiges und lohnendes Kundensegment für Mobilausrüstung aller Art ausgewiesen.

1.3.6 Netze in der Schweiz

[15]

GSM operiert in Europa vorallem in zwei Frequenzbändern, in 900 MHz und in 1800 MHz. In beiden steht ein limitiertes Spektrum zur Verfügung. Das 900er-Band wird meistens an zwei bis drei Betreiber vergeben. Dieser Bereich kann nicht weiter aufgesplittert werden, da ein qualitativ gutes Mobilfunknetz nicht in einer zu schmalen Bandbreite aufgebaut werden kann. Das gleiche passiert im 1800er-Band, welches sogar etwas breiter ist.
In der Schweiz ist man so vorgegangen, dass man dem bestehenden Mobilfunkanbieter (Swisscom Mobile) und einem neuem Bewerber (diAx) Zugang zu beiden Frequenzen verschaffte und sich der zweite Wettbewerber (Orange) auf die 1800er-Frequenz beschränkte. Damit wird jedem ein genügend grosses Stück des möglichen Bandspektrums zur Verfügung gestellt. Es wäre nicht unmöglich, Frequenzen an einen vierten Betreiber abzugeben. Je mehr Betreiber aber in den Markt drängen, desto enger würde der Spielraum und die Qualität der Netze nähme ab.

- swisscom http://www.swisscom.ch/

  900- und 1800Mhz - Netz
  2500 Antennenstandorte
  Weltweit am meisten Roamingverträge (~150 Länder/Netze)
  Netzabdeckung Swisscom (Juli 1997):

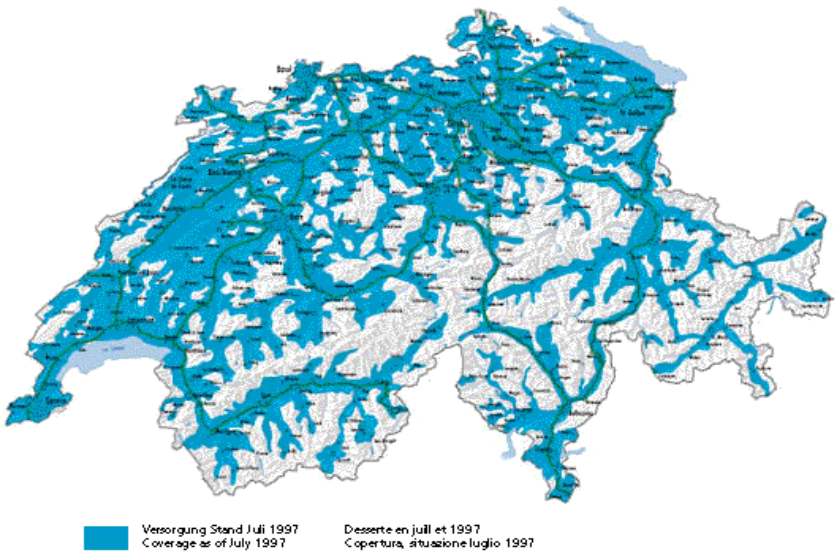


ABBILDUNG 7. Netzabdeckung Swisscom

- diAx The smart choice. http://www.diax.ch/

  900 und 1800 MHz-Netz
  Netz wurde am 24. Dezember 1998 in Betrieb genommen
  Netzabdeckung diAx (Dez. 1998):

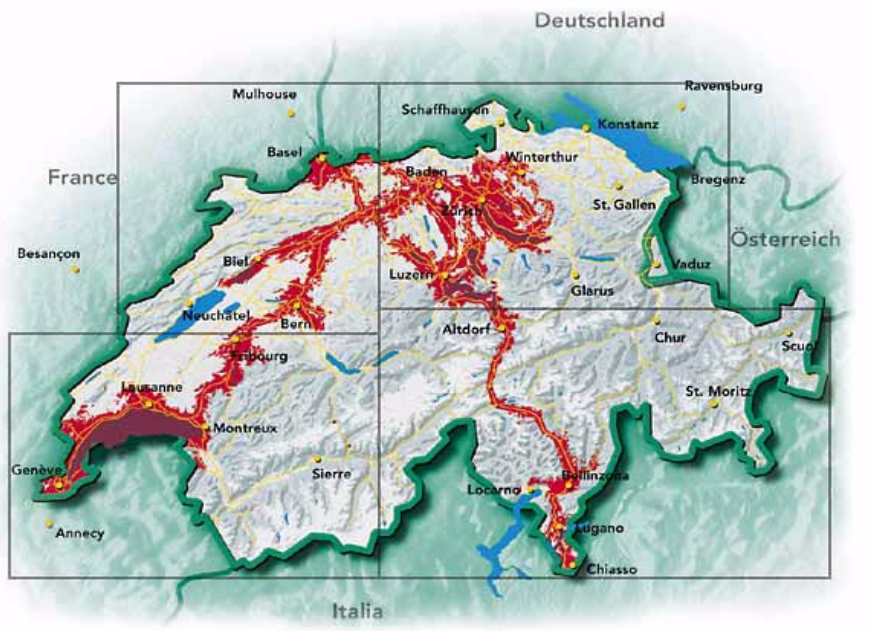


ABBILDUNG 8. Netzabdeckung diAx

Bis Ende 1999 sollten über 90% der Schweizer Bevölkerung erreichbar sein.

- orange http://ch.orange.net/d_index.html

  Zeitpunkt der Netzinbetriebnahme im Juni 1999 geplant
  1800 MHz-Netz

1.3.7 Weltweite GSM-Netzabdeckung

Weltweit gibt es über 290 GSM Provider in mehr als 100 Ländern. Falls entsprechende Abkommen zwischen den Providern existieren, ist es möglich, mit einem GSM Mobiltelefon auch auf fremden Netzen zu telefonieren. Diesen Übergang von einem Netz auf ein anderes nennt man “Roaming”. Auf der GSM-World Seite sind die aktuellen Roaming-Abkommen mit den verschiedenen GSM Providern publiziert (http://www.gsmworld.com/gsminfo/gsminfo.htm).

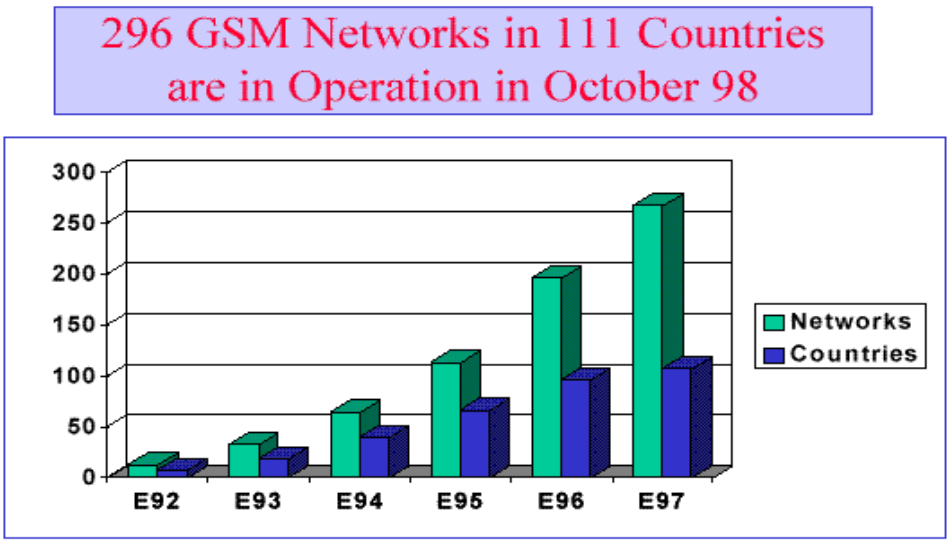


ABBILDUNG 9. GSM-Netze und Länder

1.4 Mobiltelefonmarkt

GSM Netzwerk Systeme	GSM Endgeräte (Handys)	GSM Test Systeme
Alcatel	Alcatel	Alcatel
Ericsson	Ericsson	Cray
Lucent Technologies	Mitsubishi	Racal
Motorola	Motorola	Rhode & Schwarz
Nokia	NEC	Schlumberger
Northern Telecom	Nokia	
Siemens	Panasonic	
Philips	Philips	
	Siemens	
	Sony	
	Bosch	
	Siemens	
	Sagem	
	Maxon	
	Orbitel	
	Sharp	

TABELLE 4. GSM Produktehersteller

1.4.1 Hersteller von Endgeräten

[15]

	Schweiz	Deutschland	Weltweit
1. Platz	Nokia	Siemens	Nokia
2. Platz	Motorola		
3. Platz	Ericsson		

TABELLE 5. Markaufteilung

1.4.1.1 NOKIA

Der finnische Telekommunikationsspezialist, der im breiten Publikum immer wieder als japanischer genannt wird, hat nach eigenen Aussagen bei den Endgeräten oder Terimals weltweit die Führung übernommen. Dies ist sicher das Resultat einer geschickten Modellpolitik: Für jedes Bedürfnis das richtige Gerät. Der rasche Modellzyklus erhöht zusätzlich den Druck im Markt.

1.4.1.2 MOTOROLA

Motorola erhebt den Anspruch auf einen Technologievorsprung, und dies gelingt zumindest was die Miniaturisierung betrifft. Iridium ist ein weiterer Beweis für Motorolas Technologiebewustsein. Man orientiert sich eher daran als am Design.

1.4.1.3 ERICSSON

Die Schweden ruhen sich auf welkenden Lorbeeren aus. Ericsson muss dringend seine Produktepalette rundum erneuern, um nicht den Anschluss zu verlieren. Die Markteinbussen in der Schweiz sind zu massiv, als man sie noch schönreden kann. Dual- mode lässt auf sich warten und wird, wenn es einmal da ist, kein Massenrenner. Der Hersteller ist echt gefordert.

1.4.1.4 Allgemein

Neben den grossen, bekannten Handyhersteller gibt es kleinere wie z.B. Sagem und Maxon, welche gute Geräte produzieren, denen es aber nicht gelungen ist, ein verkaufsförderndes Image aufzubereiten. Zwei deutsche und ein schweizer Hersteller haben im letzem Jahr das Hand(y)tuch geworfen: AEG, Hagenuk und Ascom produzieren keine GSM-Handys mehr. Andere werden folgen – und es würde nicht erstaunen, wenn grosse Namen darunter wären.

1.4.2 GSM Netzwerk Systeme

In der Schweiz werden vor allem von Nokia, Ericson und Philips Mobilfunknetze gebaut. Nokia bietet für Netzwerkbetreiber schlüsselfertige Netzlösungungen über die Site-Aquisation bis zum Antennenbau an und ist bestrebt, die Leaderposition zu übernehmen. In der Schweiz baut Nokia für die zwei neuen Mobilfunkanbieter diAx und Orange Netze. Das Swisscom Natel D Netz wurde vor allem von Philips und Ericson aufgebaut.

1.5 Neue Entwicklungen

[31]

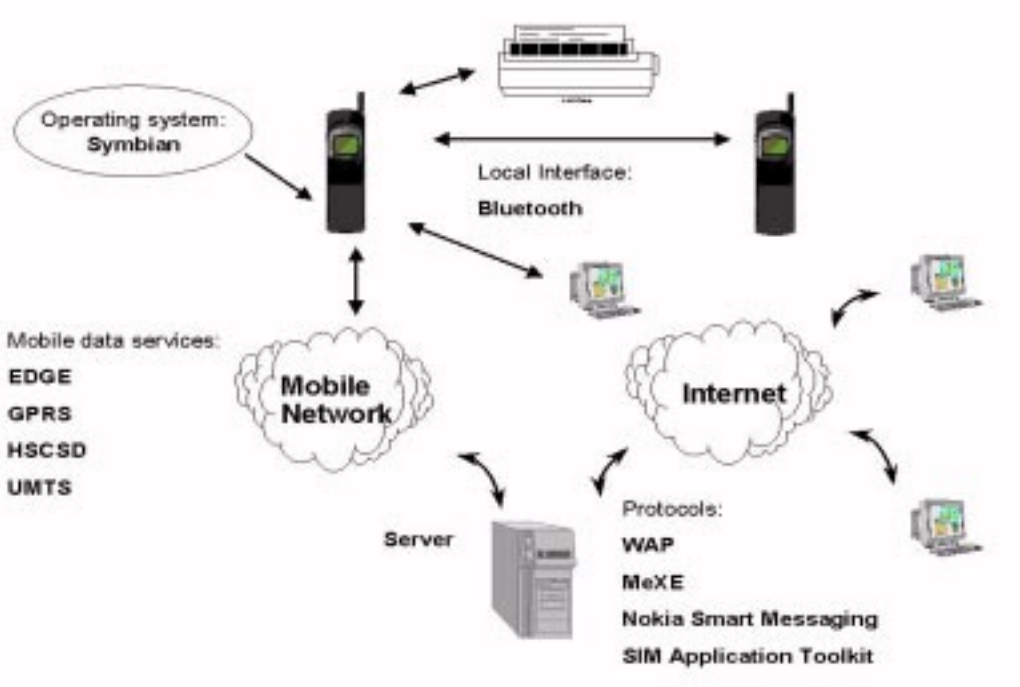


ABBILDUNG 10. Neue Entwicklungen

1.5.1 Operating Systems

1.5.1.1 Symbian

http://www.symbian.com

Mitte 1998 gründeten Nokia, Motorola und Psion Software Symbian, eine Firma die das Ziel hat, Soft- und Hardware Standards für die nächste Generation von drahtlosen Mobiltelefonen und Terminals zu entwickeln. Die Zeit, in der ein Mobiltelefon auf dem Markt ist bevor es von einem Nachfolgemodell abgelöst wird, wird immer kürzer. Deshalb werden einige Elemente in der Produkte Entwicklungsphase an andere Firmen übergeben. Zum Beispiel wurde beim Nokia 9000 Handy die Software durch die Firma Geoworks entwickelt. Ein Grund für die Gründung von Symbian war, Microsoft daran abzuhalten, ihr Windows CE Betriebssystem auf Mobiltelefone zu standardisieren. Microsoft hat schon Lizenzen an Videospiel- und Digital-TV- Produzenten vergeben. Welches System (Symbian oder Windows CE) sich durchsetzt, wird davon abhängen, zu welchem Standard am meisten Lizenzen an andere Produzenten verkaufen können.

1.5.2 Datenübermittlungsstandards

1.5.2.1 Luft-Schnittstellen

1.5.2.1.1 HIGH SPEED CIRCUIT SWITCHED DATA (HSCSD)

Im digitalen GSM-Standard wird das Zeitmultiplexierverfahren (Time Division Multiple Access, TDMA) angewandt. Die einzelnen Mobilstationen erhalten die Frequenz für die Dauer eines TDMA-Zeitschlitzes zugewiesen. Durch Vergabe von mehreren Zeitschlitzen (statt nur 1), kann die Datenübertragungsgeschwindigkeit vergrössert werden. Anstatt 14‘400 Bits pro Sekunde würde man z.B. mit 4 Zeitschlitzen eine Übertragunsrate von 57‘600 Bits pro Sekunde erreichen. Bei diesem Verfahren muss ein Kompromiss zwischen Preisfrage, verfügbare Kapazität bzw. Kanalzahl im Netz und grösserer Durchsatzrate gefunden werden. Ein Problem, das sich bei diesem Verfahren ergibt ist, dass beim Handover genau die gleichen Zeitschlitze übergeben und bis zur Beendung der Datenübertragung benutzt werden müssen.
HSCSD könnte aber einfach in einem Mobiltelefon Netzwerk implementiert werden, da es nur ein Softwareupdate der Basisstationen benötigen würde (keine neue Hardware).

1.5.2.1.2 GENERAL PACKET RADIO SERVICE (GPRS)

Im Gegensatz zu HSCSD ist GPRS eine paketorientierte Übertragung. Da bei GPRS Daten in kleinen Paketen übermittelt werden, hat GPRS Ähnlichkeiten zu SMS. GPRS benutzt die Übertragunskanäle nur dann, wenn Benutzer effektiv Daten übertragen.
Durch die effiziente Nutzung der Übertragungskanäle (bzw. den statistischen Multiplexiergewinnkönnten) könnten 50 bis 100 Benutzer die gleiche Frequenzbandbreite benutzen und von einer einzelnen Zelle bedient werden. Mit GPRS könnten Daten bis zu 170 kbit/s übertragen werden, was die zehnfache Geschwindigkeit normaler Datenübertragung ist.
Um GPRS zu implementieren, müssten Netzwerkbetreiber neue MSC und VLR installierten. Es wäre ein Aufwand, der mehrere Millionen US$ kosten würde.
Swisscom und DiAx werden GPRS in nächster Zeit einführen. Da es sich um ein strategisch wichtiges Produkt handelt, konnten uns keine Angaben gemacht werden.

1.5.2.1.3 ENHANCED DATA-RATES FOR GSM EVOLUTION (EDGE)

EDGE ist ein System, welches die Datenübertragung von GPRS auf 384‘000 bps erhöht. EDGE wurde entwickelt, um die Anforderungen an Bandbreite für Netzwerkbetreiber zu gewährleisten, welche nicht das UMTS System betreiben. Die Abteilungen von Nokia und Ericsson, welche die Netzkomponenten für Mobiltelefon Netzwerke entwickeln, bereiten sich auf EDGE vor. Es wurde bis jetzt aber kein Entscheid über EDGE kompatible Handies gefällt. Es wird erwartet, dass EDGE im Jahre 2001/2 kommerziell verfügbar sein wird.

1.5.2.1.4 UNIVERSAL MOBILE TELECOMMUNICATIONS SYSTEM (UMTS)

[19],[14]
http://www.umts-alliance.com

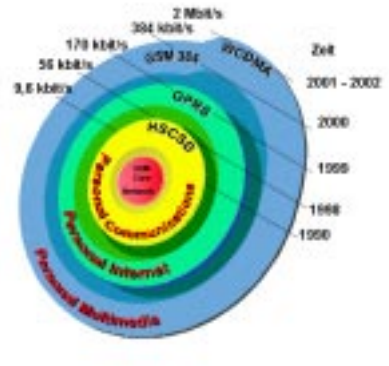


ABBILDUNG 11. Weiterentwicklung der Datenübertagung in GSM

In seiner heutigen Form eignet sich der Mobilfunk primär für Sprachverkehr, weniger für kommerzielle Datenübertragung. Schon bei der nächsten Handy- und Netzgeneration soll sich das ändern: UMTS (Universal Mobile Telecommunications Systems), die 3. Generation von Mobiltelefonen schafft voraussichtlich Übertragungsraten von bis zu 2 Megabit pro Sekunde. Mit UMTS kann künftig auch in mobilen Netzen eine komplette Palette an Sprach-, Daten und Multimedia Diensten angeboten werden. In Europa soll die Standardisierung der ersten UMTS-Phase bis Ende 1999 abgeschlossen sein. Im Jahr 2001 soll in Japan das erste UMTS-Netz nach dem breitbandigen W-CDMA-Standard in Betrieb gehen. Die Markteinführung in Europa ist zum 1. Januar 2002 geplant. Bis zur Einführung werden verschiedene Dienste der Phase 2+ wie HSCSD, GPRS oder EDGE die Datenübertragungsrate von 9,6 kbit/s kontinuierlich erhöhen.

1.5.2.1.5 Vergleich der Datenübertragungsstandards

Bezeich-nung	Maximale Übertragung srate	benötigte Zeitschlitze (Sprachkanäle)	Wahrscheinlich-keit der Einführung	Kommentar	Übertragungs-art
HSCSD	76,8 kbit/s	1 -8	klein	teuer	Zeitmultiplex
GPRS	170 kbit/s	1 -8	gross	Neue MSC müssten installiert werden	paketorientiert
EDGE	384 kbit/s		mittel	Wichtigste Förderer: Ericson, Nokia	
UMTS	2 Mbit/s		sehr gross	3. Generation	

TABELLE 6. Datenübertragungsstandards

1.5.2.2 Local Interfaces

1.5.2.2.1 Bluetooth

[26]
http://www.bluetooth.com
Bluetooth ist ein Datenübermittlungsstandard für mobile Terminals. Es ermöglicht die drahtlose Kommunikation zwischen mobilen Geräten, auch wenn keine direkte Sichtverbindung vorhanden ist.

- Gegründet durch Nokia, Ericson, IBM, Intel, Toshiba
- Über 100 Firmen sind Mittglieder der Bluetooth Alianz
- Betriebsfrequenz: 2.45 GHz global zugänglich
- 10 m Sende- / Empfangsreichweite
- Sprach- und Daten-Handling (720 kbit/s Datendurchsatz, 3 Sprachkanäle)
- 1600 Frequenzwechsel pro Sekunde kaum Interferenzprobleme
- Globale Einsatzmöglichkeiten für viele Kommunikationstechnologien
- Sende- und Empfangsmodul (Chip) ist sehr klein (9x9 mm), Integration in verschiedenste Geräte möglich
- Stromverbrauch 0,3 mA im Standby, 30 mA wenn aktiv
- Kosten: ca. Fr. 15.-- pro Chip

1.5.3 Neue Datenprotokolle

Es gibt einige neue Datenprotokolle, welche die Kommunikation zwischen Mobiltelefon und der Infrastruktur der Mobilnetzwerke (z.B. SMS-Center) intelligenter machen. Die wichtigsten Protokolle sind:

- Wireless Application Protocol (WAP)
- Mobile Station Application Execution Environment (MexE)
- Nokia Smart Messaging
- SIM Application Toolkit

1.5.3.1 Wireless Application Protocol (WAP)

http://www.wapforum.org

WAP ist ein Standard welcher definiert, wie Daten vom Internet gefiltert werden müssen, damit sie für die Mobilkommunikation benutzbar sind.

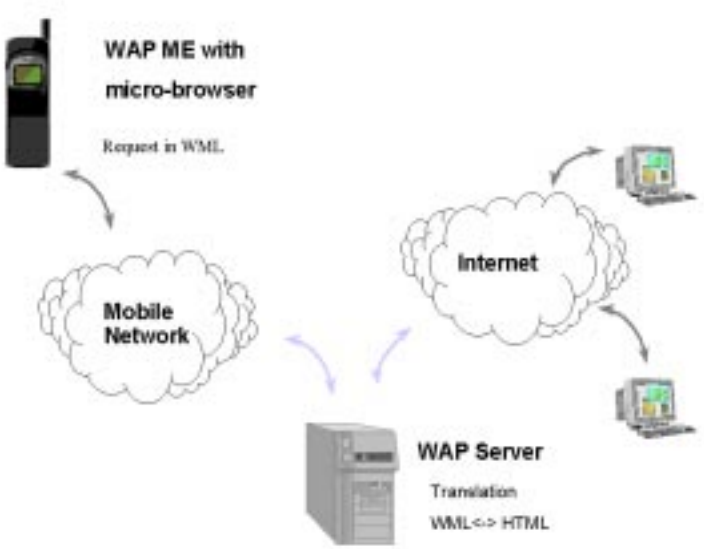


ABBILDUNG 12. Wireless Application Protokol (WAP)

- Beteiligte Firmen: Motorola, Nokia, Ericsson, Unwired Planet, Schlumberger, Certicom
- Funktioniert in den verschiedenen Mobilnetzwerken (CDMA, GSM, UMTS)
- Erweitert und fasst die drahtlosen Datenprotokolle (Nokia Smart Messaging, UPLink) zusammen.
- Benutzt einen neuen HTML Standard: WML (Wireless Markup Language)
- Smartcard wird bei diesem Protokoll nicht speziell eingesetzt
- Protokoll nicht für Applikationen wie mobile banking benutzbar, da nicht sicher
- Micro Browser im Mobiltelefon
- Philosophie von WAP ist, möglichst wenig Ressourcen am Mobiltelefon zu benutzen, dafür die Funktionalitäten der Netzwerkes auszunützen.

1.5.3.2 Mobile Station Application Execution Environment (MeXE)

[31]

Ziel von MeXE ist, eine umfassende und standardisierte Umgebung für Mobiltelefone zur Verfügung zu stellen. MeXE übertrifft die Funktionen von WAP und stellt eine hochentwickelte Umgebung für Übermittlungen, Programmierung und Interface design zur Verfügung.

- Entwicklung durch Lucent Technologies und NorTel in Großbritannien
- Java Virtual Machine in Mobiltelefon eingebaut
- Benötigt grosse Prozessorleistung, da Java Applikationen benutzt werden
- MexE Dienste sind entwickelt worden, damit sie Spracherkennung, Icons und Softkeys unterstützen
- Softwareapplikationen können auf dem Mobiltelfon abgespielt werden

1.5.3.3 Nokia Smart Messaging

Smart Messaging ist ein geschütztes protokoll von Nokia, welches es ermöglicht, Informationen zwischen Mobiltelefonen und jeglichen Informationsquellen auszutauschen.

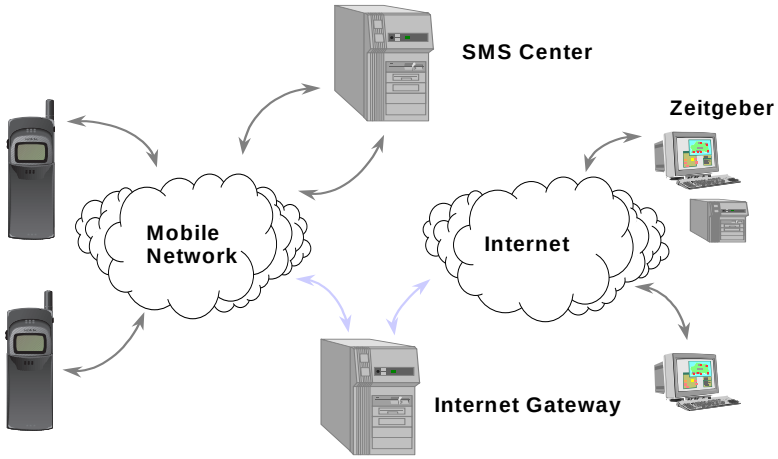


ABBILDUNG 13. Nokia Smart Messaging

- Client-Server Lösung
- Integriert im Nokia 8110i und Nokia 9000i (z.B. zum Versenden von Visitenkarten)
- Implementierung in TTML (Tagged Text Markup Language)
- HTML wird in TTML übersetzt, was die Übertragung der Information als SMS erlaubt
- Update der Menüs im Mobiltelefon mit SMS möglich
- Dienste können Telefonnummern ans Mobiltelefon senden, welche automatisch im Telefonverzeichnis eingetragen werden
- Nachteil: Nur einige Nokia Mobiltelefone unterstützen diesen Standard, andere Mobiltelfonhersteller nicht. Das Heisst, es handelt sich um eine proprietätre Lösung.

1.5.4 SIM Application Toolkit

[9]

ABBILDUNG 14. SIM Application Toolkit

Mit dem SIM Application Toolkit haben Netzwerkanbieter Zugriff zur SIM-Karte (siehe 3.0 Subscriber Identity Module (SIM)) und können sie updaten oder umprogrammieren. Es können auch mittels SMS neue Dienste auf die Karte heruntergeladen werden.
Das SIM Application Toolkit auf der SIM-Karte ist völlig getrennt von den anderen GSM Funktionen der SIM-Karte. Der Toolkit benutzt andere Befehle. Deshalb ist es möglich, dass der SIM-Toolkit und das Mobiltelefon miteinander kommunizieren, während die GSM Kommunikation zwischen SIM-Karte und Mobiltelefon stattfindet. Die Kommunikation zwischen dem Toolkit und Server des Netzwerkes erfolgt zur Zeit mittels SMS. In Zukunft werden andere Transportmechanismen wie USSD (Unstructured Supplementary Services Data strings) oder GPRS verwendet werden.

Mittels SIM-Toolkit können 21 Befehle von der SIM-Karte an das Mobiltelefon geschickt werden. Hier sind sie nach Empfänger geordnet.

SIM-GSM Benutzer Befehle:

Diese Befehle ermöglichen den Informationsaustausch mit dem Benutzer

- **DISPLAY TEXT** Text oder Icon (falls unterstützt) wird auf dem Mobiltelefon anzeigen.
- **PLAY TONE** Mobiltelefon spielt Ton auf Lautsprecher.
- **GET INKEY** Text oder Icon (falls unterstützt) wird auf dem Mobiltelefon angezeigt und es wird auf eine Tasteneingabe gewartet.
- **GET INPUT** Text oder Icon (falls unterstützt) wird auf dem Mobiltelefon angezeigt und es wird auf eine Eingabe gewartet (auch mehrere Character).
- **SELECT ITEM** SIM stellt eine Liste von verschiedenen Posten dar, aus dem der Benutzer wählen kann.
- **SET UP MENU** SIM liefert eine Liste von Posten, die in der Mobiltelefon Menü-Struktur implementiert werden sollen.

SIM-NETZWERK Befehle

Mit diesen Befehlen kann die SIM-Karte das ME anweisen mit dem Netzwerk zu kommunizieren

- **SEND SHORT MESSAGE** SMS oder SMS-COMMAND wird an Netzwerk gesendet.
- **SEND SS** Ein SS Gesuch wird an das Netzwerk gesendet.
- **SEND USSD** Ein USSD string wird an Netzwerk gesendet.
- **SET UP CALL** Es werden 3 verschiedene Anruftypen unterschieden:
  - Anruf durchstellen, aber nur falls Mobiltelefon zur Zeit nicht benutzt wird
  - Anruf durchstellen, und alle anderen Anrufe in die Warteschlange stellen
  - Anruf durchstellen, und alle anderen Anrufe abhängen

- **PROVIDE LOCAL INFORMATION** Mobiltelefon wird gebeten, lokale Informationen an SIM zu schicken. Z.B: Land in dem sich das Mobiltelefon befindet oder Netzwerk Codes (MCC + MNC).

SIM-ME Befehle

- **REFRESH** Mobiltelefon wird gebeten, SIM Initialisation gemäss GSM 11.11 durchzuführen und/oder es wird dem Mobiltelefon mitgeteilt, dass der Inhalt oder die Struktur von EFs auf der SIM-Karte verändert worden sind. Mit diesem Befehl ist es auch möglich, einen Reset der SIM auszuführen.
- **MORE TIME** SIM-Karte bittet Mobiltelefon um Zeit, Prozesse auszuführen
- **POLL INTERVAL** Stellt fest, wie oft das Mobiltelefon den STATUS-Befehl während des idle modus an die SIM gesendet hat.
- **SET UP EVENT LIST** SIM stellt Liste mit Ereignissen zusammen, und will vom Mobiltelefon Informationen über diese erhalten, falls sie eintreten.
- **TIMER MANAGEMENT** Timer wird für eine bestimmte Zeit aktiviert (Nur falls Timer unterstütz wird)
- **POLL OFF** Proactive Polling (in GSM 11.11 definiert) wird ausgeschalten

Befehle, die nur gültig sind, falls Mobiltelefon mehrere Kartenschächte *1*) hat:

- **GET READER STATUS** Befehl wird benutzt, um Informationen über weitere Karten zu erhalten.
- **PERFORM CARD APDU** Befehl bittet Mobiltelefon, APDU Befehl an zweite Karten weiterzuleiten.
- **POWER OFF CARD** Beendet Session mit weiteren angeschlossenen Karten
- **POWER ON CARD** Session mit 2. angeschlossener Karte wird begonnen. Alle ATR bytes werden retourniert.

Mit diesen Befehlen ist es möglich folgende Funktionen auszuführen:

- Daten vom Netzwerk auf das SIM laden, wobei eine SMS-Meldung direkt vom Netzwerk an die SIM-Karte geschickt wird. Dieses SMS kann Daten oder Befehle beinhalten, um neue Applikationen auf der SIM zu laden.
- SMS von der SIM ans Mobiltelefon verschicken, und Befehl ans Telefon geben, SMS weiterzuleiten.
- “Anrufkontrolle”: Alle gewählte Nummern werden durch das SIM geleitet. Sie können dort geprüft, modifiziert oder sogar abgeblockt werden.
- Es kann eine SMS vom Netzbetreiber an die SIM-Karte geschickt werden. Dadurch ist es möglich, Einträge in das Adressbuch des Benützers zu machen.

Eine Vielzahl von Applikationen wird in Zukunft mit SIM-Application Toolkit möglich sein:

- Mobile banking
- Flugreservationen
- Anfrangen an verschiedene Datendienste

1) Prototypen für Testzwecke

Handy's die diesen Standard unterstützen:

- Philips Genie
- Motorlola CD920, CD930, D 520
- Alcatel One Touch Easy
- Siemens S10 Active
- Ab April 1999 Siemens C25
- Ab Juli 1999 Siemens S25

1.5.4.1 Sicherheitsmechanismen für SIM Applikation Toolkit

[10], [11]

Kommunikation im GSM Netzwerk, welche mit SIM Application Toolkit in Verbindung steht, kann durch den Netzwerkanbieter oder den SIM Toolkit Dienstanbieter gesichert werden.
Die Sicherheitsmechanismen für SIM Applikation Toolkit erfüllen die folgenden Sicherheitserforderungen:

- Echtheit derKommunikationspartner (SIM und Netzwerk)
- Echtheit der Meldung
- Antwortdetektion
- Nachweis des Empfangs und Bestätigung der Ausführung
- Vertraulichkeit einer Nachricht

Erläuterung zu Abbildung 15

- Sending Application: Die Einheit, die eine Applikationsmeldung generiert, die verschickt werden soll.
- Sending Entity: Einheit, die gesicherte (secured) Pakete generiert (SMS-SC, SIM, SIM, Toolkit Server).
- Receiving Entity: Die Einheit, die die gesicherten Pakete empfängt und den Sicherheitsmechanismus anwendet.
- Receiving Application: Applikation, an die die Meldung gerichtet ist.

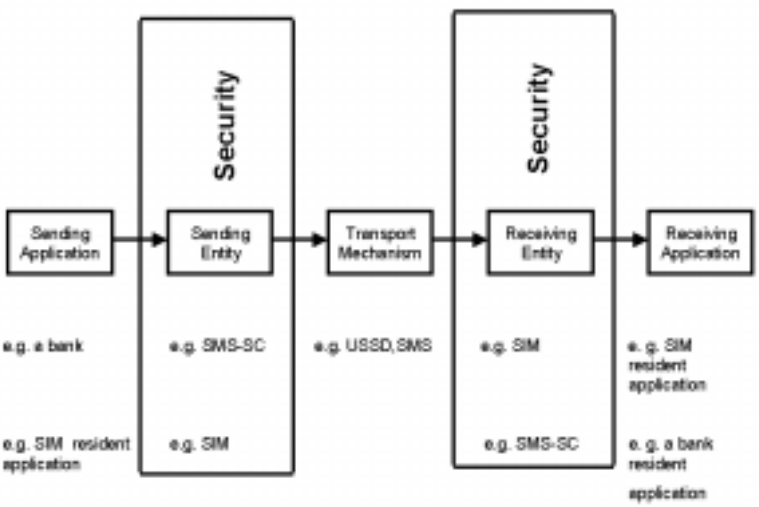


ABBILDUNG 15. Sicherheitsübersicht

Die Applikation, die verwendet wird, um Meldungen zu versenden (Sending Application) schickt eine Applikationsmeldung an die Sendeeinheit (Sending Entity). In der Meldung ist vermerkt, wie die Sicherheit an die Meldung angewandt werden soll.
Die Sendeeinheit fügt einen Sicherheitsheader an die Applikationsmeldung an.
Unter normalen Umständen wird der Sicherheitsheader von der Empfangseinheit (Receiving Entity) empfangen. Die Meldung wird gemäss dem Sicherheitsheader decodiert und der Empfangsapplikation (Receiving Application) weitergegeben. Der Empfangsapplikation wird mitgeteil, was für Sicherheit angewandt wurde.

Die Sicherheitserforderungen, die erfüllt werden müssen, um Applikationen vom Sending Entity zum Receiving Entity zu übertragen sind:

Authentifizierung

- Echtheit der Meldung
- Antwortdetektion
- Nachweis des Empfangs und Bestätigung der Ausführung
- Vertraulichkeit einer Nachricht
- Anzeige der angewandten Sicherheitsmechanismen

Die Sicherheitsmechanismen werden für jedes übertragene Paket angewandt. Es besteht die Möglichkeit, den Mechanismus ein- und auszuschalten.

Möglichkeiten der Sicherheitsmechanismen auf dem Transport Layer:

- Authentifizierung
  - Kryptographische Prüfsumme
  - Digitale Unterschrift
- Echtheit der Meldung
  - Redundanz Prüfung
  - Digitale Unterschrift
- Antwortdetektion
  - Einfacher Zähler
  - Ein Zähler, der in der Kalkulation der Kryptographischen Prüfsumme enthalten ist
  - Ein Zähler, der in der Kalkulation der digitalen Unterschrift enthalten ist
- Nachweis des Empfangs und Bestätigung der Ausführung
  - Ungesichertes Acknowledgement
  - Acknowledgement, welches in der Kalkulation der Kryptographischen Prüfsumme enthalten ist
  - Acknowledgement das in der Kalkulation der Digitalen Unterschrift enthalten ist
- Vertraulichkeit einer Nachricht
  - Verschlüsselungsmechanismus

1.5.5 Vergleich der Datenprotokolle

Neue Entwicklung	Wahrscheinlichkeit der Einführung	Kommentar
SIM Application Toolkit	klein	Sicher, kann für mobile Banking verwendet werden
Nokia Smart Messaging	klein	Nur durch Nokia Mobiltelefone unterstützt
WAP	gross	Funktioniert in CDMA, GSM, UMTS Netze
MExE	mittel	Nur GSM Standard

TABELLE 7. Vergleich der Datenprotokolle

1.6 GSM Normierung

1.6.1 Phase 1

GSM ist kein abgeschlossenes System, das sich nicht mehr verändert. Die GSM-Standards werden laufend weiterentwickelt. Die Phase 1 der Implementierung von GSM-Systemen beinhaltete grundlegende Telematikdienste. Allen voran Sprachkommunikation und einige wenige Zusatzdienste, die zur Markteinführung von GSM 1991 verbindlich von allen Netzbetreibern angeboten werden konnten. Die Einführung der Phase 1 Systeme GSM 900 und DCS 1800 erfolgte 1991 bzw. 1993.

Art der Dienste	Dienst
Telematikdienste	Ferngespräche Notrufe Fax Gruppe 3 SMS
Trägerdienste	Daten asynchron 300...9600 bit/s
Zusatzdienste	Anrufweiterleitung

TABELLE 8. Phase 1 Dienste

1.6.2 Phase 2

In der Phase 2, deren Standardisierung 1995 abgeschlossen wurde und deren Markteinführung auf breiter Front im Jahr 1996 erfolgte, nahm die ETSI vor allem Zusatzdienste in den Standard auf. Mit diesen bereits von Anfang der GSM-Entwicklung an geplanten Zusatzdiensten wurden Leistungsmerkmale implementiert, wie sie aus dem Festnetz-ISDN bekannt sind. Alle Netze und Endgeräte der GSM Phase 2 wahren allerdings die Kompatibilität zu den alten Endgeräten der GSM Phase 1, d.h. alle neuen Standardentwicklungen geschahen unter strengen Vorgaben der Abwärtskompatibilität.

Art der Dienste	Dienst
Zusatzdienste	Rufnummernanzeige
	Anklopfen und Halten
	Konverenzschaltung
	advice of charge 1)
	half rate speech codec 2)
	Verbindungen sperren

TABELLE 9. Zusatzdienste Phase 2

1) Gebührenanzeige
2) Sprachcodec der halben Bitrate

1.6.3 Phase 2+

Bei der Phase 2+ handelt es sich um die zeitlich offene, nicht durch Zielvorgaben und Einführungszeitpunkte abgeschlossene, Evolution von GSM-Systemen. In Angriff genommen wird eine breite Palette technischer Aspekte. Es muss betont werden, dass es sich dabei um geplante und in der Standardisierungsdiskussion befindliche Dienste handelt – eine tatsächliche Implementierung ist dabei noch nicht gesichert. Es stehen über 80 Einzelthemen zur Diskussion.

Beispiele zu neuen Phase 2+ Dienste:

- HSCSD
- Paketdienst GPRS
- Gebührenzählung
- Verbesserung der Sprachqualität durch Weiterentwicklung der Sprachdienste
- SIM Application Toolkit
- EDGE
- MeXE

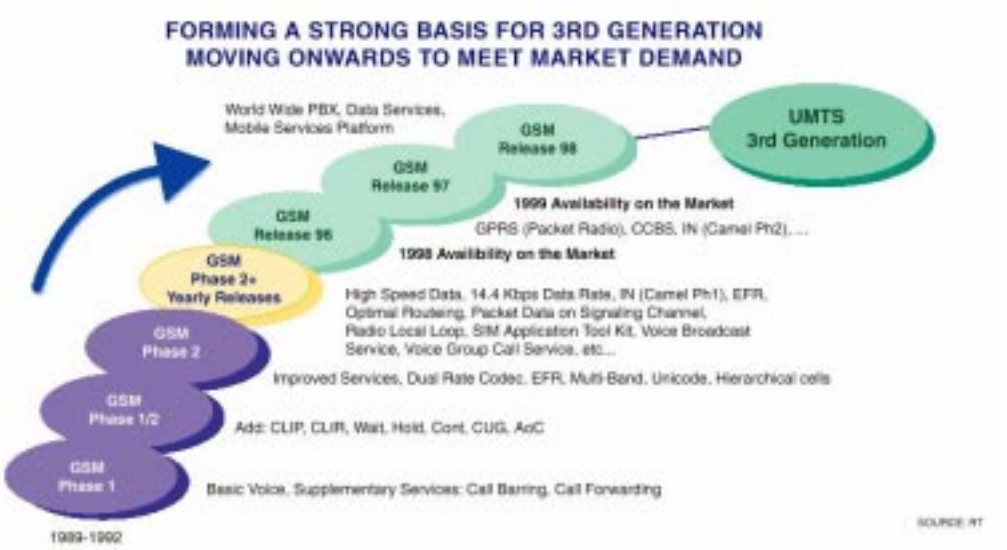


ABBILDUNG 16. Weiterentwicklungen

2.0 GSM Technik

2.1 Architektur des GSM Netzes

[1],[4],[29]

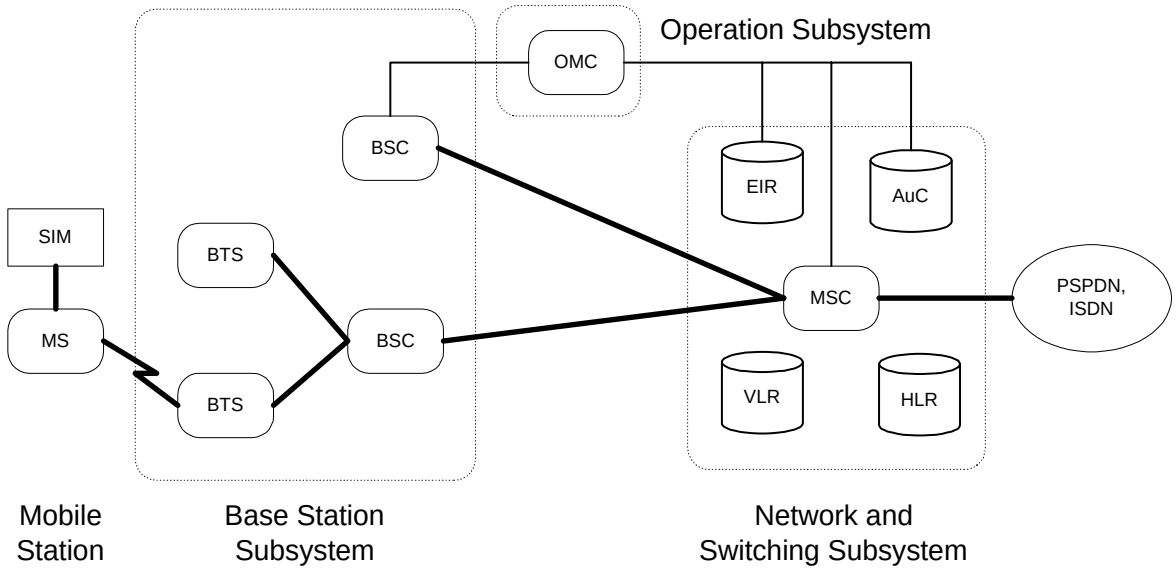


ABBILDUNG 17. Architektur eines GSM-Netzes

Das GSM System hat zwei wesentliche Bestandteile: die fest installierte Infrastruktur (Netz im eigentlichen Sinn) und die Mobilteilnehmer, welche über die Funk- oder auch Luftschnittstelle (air interface) die Dienste des Netzes nutzen und kommunizieren. Das fest installierte GSM-Netz wiederum kann in drei Subnetze untergliedert werden: das Funknetz, das Mobilevermittlungsnetz und das Managementnetz. Diese Netze werden in den GSM-Empfelungen (GSM-Rec. 03.04) als Subsystem bezeichnet.

Die drei entsprechenden Subsysteme sind:

- Base Station Subsystem (BSS)
- Network and Switching Subsystem (NSS)
- Operation Subsystem (OSS)

Die Mobile Station (MS) wird vom Abonnenten getragen oder in einem Fahrzeug mitgeführt. Das BSS kontrolliert die Funkverbindung der MS mit dem Netzwerk, das NSS ist für die Verbindung zum Festnetz oder anderen Mobilnetzen verantwortlich, und schliesslich wird das Ganze vom OSS kontrolliert.

2.1.1 Mobile Station

Die Mobile Station (MS) ist der einzige Teil des GSM Netzes den der Abonnent im Allgemeinen zu sehen bekommt. Sie besteht aus zwei Teilen: dem Gerät selbst (mobile equipment, ME) auch Natel oder Handy genannt und einer SIM-Karte (Subscriber Identity Module, SIM). In jedem ME ist eine IMEI (International Mobile Equipment Identity) Nummer gespeichert über die jedes Handy eindeutig identifiziert werden kann. Jede SIM-Karte beinhaltet eine Nummer, die IMSI (International Mobile Subscriber Identity) mit der das System den Abonnenten eindeutig identifizieren kann.

Anhande der IMSI Nummer ist es dem Netzbetreiber möglich die Kosten zu verrechnen. Im Weiteren kann die SIM-Karte mit einem Personal Identity Number (PIN) gegen unautorisierten Zugriff geschützt werden.

Durch das konsequent angewendete Konzept des SIM wird zum einen eine Trennung von Benutzermobilität und Gerätemobilität erreicht.

2.1.2 Subscriber Identity Module

Das Subscriber Identity Module ist als fest eingebauter Chip (Plug-In SIM) oder als austauschbare Chipkarte realisiert. Auf ihr werden verschiedene Daten (z.B. IMSI, MSISDN, eigene Telefonnummern,...) gespeichert (siehe 3.0 Subscriber Identity Module (SIM)).

2.1.3 Base Station Subsystem

Das Base Station Subsystem (BSS) ist die Funkkomponente des GSM-Netzes. Sie ermöglicht die Kommunikation mit den MS in einem bestimmten, in Zellen unterteilten Bereich des Netzes. Das BSS stellt die Funkkanäle für Signalisierung und Nutzverkehr zur Verfügung. Es besorgt auch die Fehlerschutzcodierung und –decodierung für die Funkkanäle. Im Weiteren stellt das BSS die Verbindung mit dem Mobile Switching Center (MSC) her. Die Verbindung zwischen BSC und MSC ist genormt und erfolgt über ein sogenanntes A-Interface. Dies ermöglicht es Geräte von Verschiedenen Herstellern zu verwenden. Für die Verbindung zwischen BSC und MSC werden typischerweise Mietleitungen verwendet. Typische Datenraten sind hier 2048 kbit/s oder 64 kbit/s (ITU-T G.703, G.705, G.732).

Das BSS beinhaltet:

- eine oder mehrere Base Transiver Stations BTS
- einen Base Station Controller BSC

Die BTS beinhaltet die Funkkomponenten die für die Funkverbindung mit der MS verantwortlich sind. Die Reichweite einer solchen BTS liegt nominell bei bis zu 37.8km (GSM) Radius, fällt in der Praxis jedoch je nach Geländesituation (bzw. Reflexionen und Dämpfung) deutlich geringer aus. Da viele kleine Zellen in Ballungsgebieten mehr Teilnehmer pro Fläche versorgen können, als wenige grosse, arbeiten viel Netzbetreiber absichtlich mit kleineren Zellen, indem sie Richtantennen (Sektoren) einsetzen und/oder mit niedrigem Leistungspegel senden.

Eine BSC kontrolliert eine oder mehrere BTS und wirkt als Digital-Verarbeitung-Schnittstelle zum Rest des Netzes. Die Verbindung von BTS zu BSC erfolgt via Richtstrahlverbindung oder seperater Leitung. Typische Datenrate auf dieser Verbindung sind 2048 kbit/s oder 64 kbit/s (ITU-T G.703, G.705, G.732). Die Hauptfunktionen der BSC bestehen darin Funkkanäle und Kontrollnachrichten zur oder von der MS zu organisieren. Träger- und Kontrollkanäle sind immer unter der Kontrolle der BSC. Dies heisst aber nicht das auch alle Nachrichten in der BSC verarbeitet werden. In vielen Fällen dient die BSC nur als Verbindungsglied zur MSC oder zur MS.

2.1.3.1 Maximale Reichweite einer BTS

Der relativ suspekt erscheinende Wert der maximalen Reichweite einer GSM-Basisstation berechnet sich aus der Länge der “Guard Period” in den Zugriffsdatenblöcken (“Access Burst”), wie sie zwischen MS und BTS gesendet werden.
Ein Zeitrahmen dauert 4,615ms und umfasst 8 Zeitschlitze, ein einzelner Zeitschlitz dauert somit 0,576875ms. Während eines solchen Timeslots wird ein "Normal Burst" übertragen, der aus 156,25 Bit Daten besteht. Ein Bit wird demnach in 3,692 Mikrosekunden gesendet.
Der erwähnte Access Burst verwendet nun eine Schutzzeit von 68,25 Bit für die Synchronisation mit der Gegenstelle, wodurch Laufzeitunterschiede bis zu

0,5 * 68,25 * 3,692 Mikrosekunden = 0,1259895 ms

ausgeglichen werden können. Wie man aus dem Physikunterricht weiss, breiten sich elektromagnetische Wellen mit Lichtgeschwindigkeit (300000 km/s) aus. Demnach darf die maximale Entfernung

0,1259895E-03 s * 3E8 m/s = **37796,85 m**

nicht überschreiten.

(siehe auch „2.4.1.3 Anwendung im GSM“ auf Seite 40)

2.1.3.2 Network and Switching Subsystem

Das Network and Switching Subsystem (NSS) besteht aus den Mobilvermittlungszentralen (MSC) mit den Datenbanken, welche die zur Vermittlung und Diensterbringung notwendigen Daten speichern. Die zentrale Komponente des NSS ist das Mobile Switching Center (MSC). Das MSC arbeitet wie eine normale Schaltzentrale im PSTN oder ISDN besitzt aber diversen Zusatzfunktionen. Die MSC liefert verschiedene Funktionen für die Handhabung von Abonnenten wie Registration, Identifikation, location updating und Handover.

Die Bestandteile sind:

- Mobile Switching Center (MSC)
- Home Location Register (HLR)
- Visited Location Register (VLR)
- Equipment Identity Register (EIR)
- Authentication Center (AuC)

2.1.3.3 Mobile Switching Center

Ein MSC ist der Vermittlungsknoten des GSM-Netzes und erfüllt alle vermittlungstechnischen Funktionen eines Festnetzvermittlungsknoten, wie z.B. Wegsuche oder Signalwegschaltung. Der Hauptunterschied zu einem normalen ISDN-Vermittlungsknoten ist , dass eine MSC die Zuteilung und Verwaltung von Funkressourcen und die Mobilität der Teilnehmer zu berücksichtigen hat. Die BSC eines BSS unterstehen jeweils eindeutig eienm MSC.
Zur Ein- und Auskopplung des Gesprächsverkehrs in und aus dem Festnetz stehen GMSC (Gateway MSC) zur Verfügung.

2.1.3.4 Home Location Register

Das HLR ist eine Datenbank die für die Teilnehmerregistrierung und –lokalisierung verantwortlich ist. Im allgemeinen ist je PLMN (Public Land Mobile Network) ein zentrales HLR vorhanden. Das HLR ist das Heimatregister, das jeden Teilnehmer (IMSI) und jede MSISDN-Rufnummer registriert, die in seinem Netz "beheimatet" ist. Zu den gespeicherten Daten gehören neben festen Einträgen, wie abonnierte Dienste und Berechtigungen, vor allem auch ein Verweis auf den aktuellen Aufenthaltsort einer Mobilstation. Das HLR wird zur Wegsuche für Rufe zu von ihm verwalteten Mobilteilnehmern verwendet.

2.1.3.5 Visited Location Register

Das Besucherregister Visited Location Register (VLR) ähnelt sehr dem HLR, ausser dass es normalerweise mehrmals in einem GSM-Netz vorkommt, nämlich meist eins pro MSC. Ein VLR verwaltet also die Daten aller MS, die sich momentan im Verwaltungsbereich des zugehörigen MSC aufhalten. Ein VLR kann aber auch für mehrere MSC verantwortlich sein.
Beim Betreten einer neuen Local Area (LA) startet ein MS jeweils eine Registrierungsprozedur. Das zuständige MSC leitet dabei die Identität der MS und ihre momentane Local Area Identity (LAI) an das VLR weiter, die diese Daten bei sich einträgt und die MS so registriert. Wenn die MS noch nicht in diesem VLR registriert war, wird das HLR über den aktuellen Aufenthaltsort der MS informiert. Dabei werden Daten übermittelt, welche die Wegsuche für Rufe zu den MS ermöglichen.

2.1.4 Operation Subsystem OSS

Der laufende Netzbetrieb wird mit dem Operation Subsystem gesteuert und gewartet. Steuerfunktionen des Netzes werden vom Operation and Maintenance Center OMC überwacht und ausgelöst.

Zu den Funktionen gehören:

- Verwaltung und kommerzieller Betrieb (Teilnehmer, Endgeräte, Abrechnung,..)
- Sicherheitsmanagement
- Netzfunktionen, Netzbetrieb und Performance Management
- Wartungsarbeit

Im GSM sind neben HLR und VLR zwei weitere Datenbanken zur Systemsicherheit definiert. Vertrauliche Daten zur Teilnehmeridentifikation und Schlüssel werden im Authentication Center AuC gespeichert bzw. erzeugt. Die Schlüssel dienen zur Benutzerauthentifizierung und autorisieren den jeweiligen Dienstzugang. Das Geräteregister Equipment Identity Register EIR speichert die Seriennummern der Endgeräte (IMEI), so dass z.B. einem als gestohlen gemeldeten Endgerät der Dienstzugang gesperrt werden könnte.

2.2 Zellulartechnik

[4],[27]

2.2.1 Grundbegriffe

Einem Mobilfunknetz stehen aufgrund der sehr begrenzten Frequenzbänder nur eine relativ kleine Anzahl von Gesprächskanälen zur Verfügung. Beispielsweise sind dem GSM System 25 MHz Bandbreite um 900 MHz zugeteilt, so dass bei einer KIanalbandbreite von 200 kHz maximal 125 Frequenzkanäle zur Verfügung stehen, womit man durch eine achtfach Zeitmultiplex auf 1000 Datenkanäle kommt.
Um trotzdem die grosse Zahl von Teilnehmern zu bewältigen müssen die Frequenzen (geographisch) mehrfach genutzt werden. Um diese Anforderung zu erfüllen wurde die Zellulartechnik entwickelt, mit der eine deutlich verbesserte Frequenzökonomie erzielt wird.

Charakteristiken dieses Verfahrens:

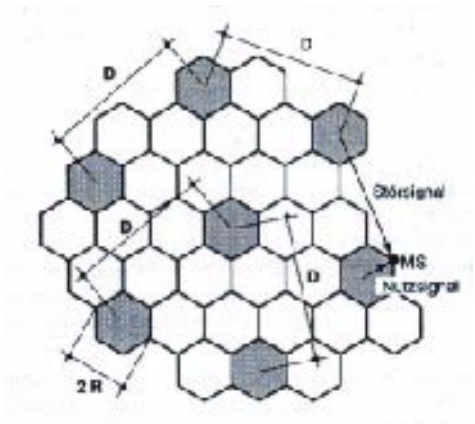


ABBILDUNG 18. Zellen als Hexagone

•Gebiet wird in Zellen (einzelne Funkzonen) aufgeteilt (Hexagone).
•Jede Zelle y erhält eine Untermenge von Frequenzen fb_y aus der im Mobilnetz verfügbaren Gesammtmenge zugeteilt. Zwei benachbarte Zellen dürfen nicht dieselben Frequenz verwenden da es sonst zu Gleichkanalstörungen käme.
•Die Frequenzen aus dem Bündel fb_y dürfen erst in einem Abstand D (Frequenzwiederholabstand) wieder verwendet werden.
•Beim Übergang von einer Zelle zur Nächsten erfolgt bei laufendem Gespräch ein automatischer Kanal-/Frequenzwechsel (Handover), welcher in der Regel nicht wahrgenommen wird.

2.2.2 Clusterbildung

[4]

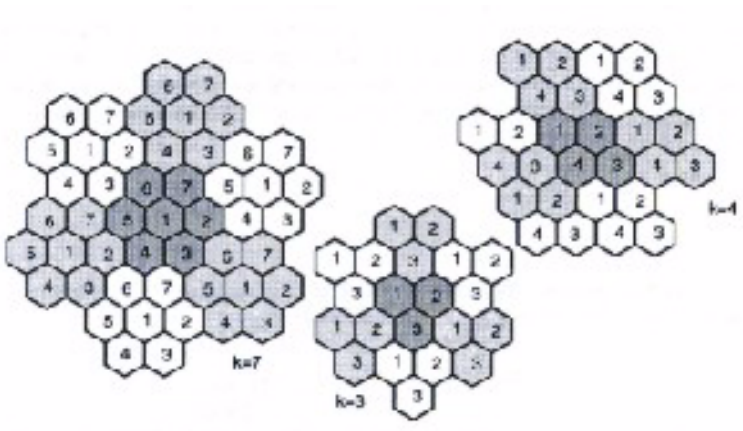


ABBILDUNG 19. Zellcluster

Die regelmässige Wiederholung der Frequenzen hat eine Gruppierung der Zellen zur Folge. In einer solchen Gruppe (Cluster) können alle im Netz verfügbaren Frequenzen enthalten sein. Die Anzahl, in einem Cluster vorhandenen Zellen, k ist ein Mass für den Frequenzwiederholabstand D.

Für ein Cluster gilt:

- Alle Frequenzen des Netzes können enthalten sein.
- Keine Frequenz wird mehrfach genutzt.

Je grösser ein Cluster, desto grösser wird D und desto grösser der Signal-Störabstand.
Je grösser k, desto geringer jedoch die Anzahl von Kanälen und damit die Teilnehmerzahl je Zelle.

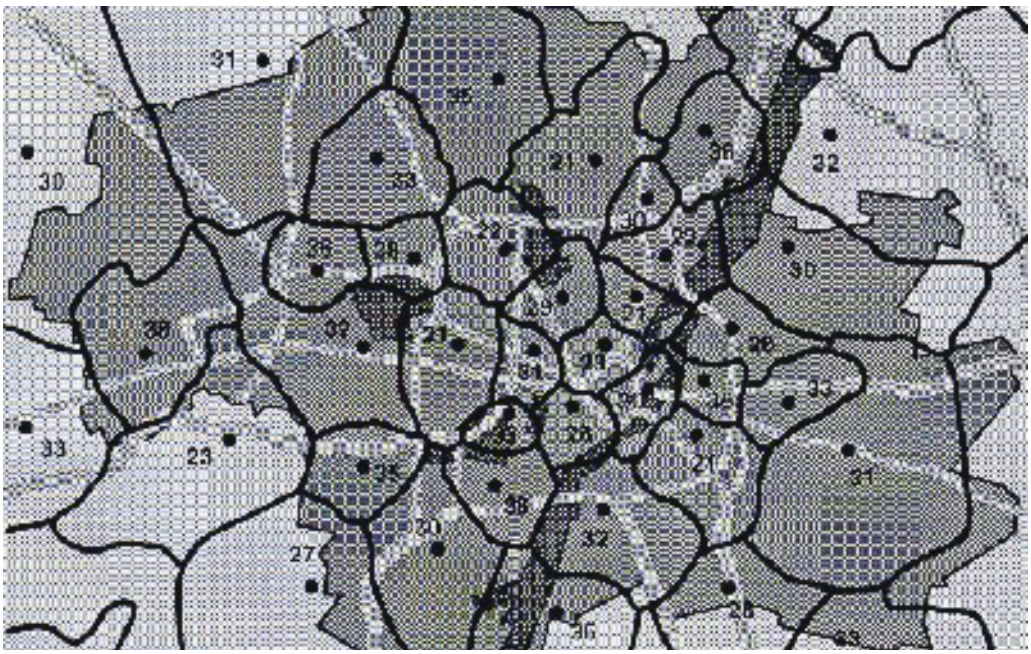


ABBILDUNG 20. Reale Zelleinteilung

Die bisher gezeigte Gliederung und Einteilung eines Gebietes in Hexagonale-Zellen ist sehr idealisiert. In der Realität sind Zellen keines Wegs hexagonal, sie besitzen vielmehr sehr unregelmässige Formen und verschiedene Grössen.

2.3 Adressen und Kennziffern

[4]

Im GSM-Netz wird klar zwischen Benutzer und Gerät unterschieden und beides voneinander getrennt. Mobilgerät und Benutzer erhalten so jeweils eine international eindeutige Kennziffer. Die Benutzeridentität wird auf einer SIM-Karte (Subscriber Identity Module) gespeichert. Diese SIM ist portabel und so zwischen verschiedenen Endgeräten transferierbar. Zusätzlich wird zwischen Teilnehmeridentität und Rufnummer unterschieden. Neben einer persönlichen Kennziffer erhält also jeder GSM-Teilnehmer eine (oder auch mehrere) ISDN-Rufnummer zugeteilt. Neben den bereits erwähnten Nummern sind noch weitere definiert, die zur Handhabung der Teilnehmermobilität und der Adressierung der übrigen Netzkomponenten benötigt werden. Die wichtigsten werden im folgenden vorgestellt.

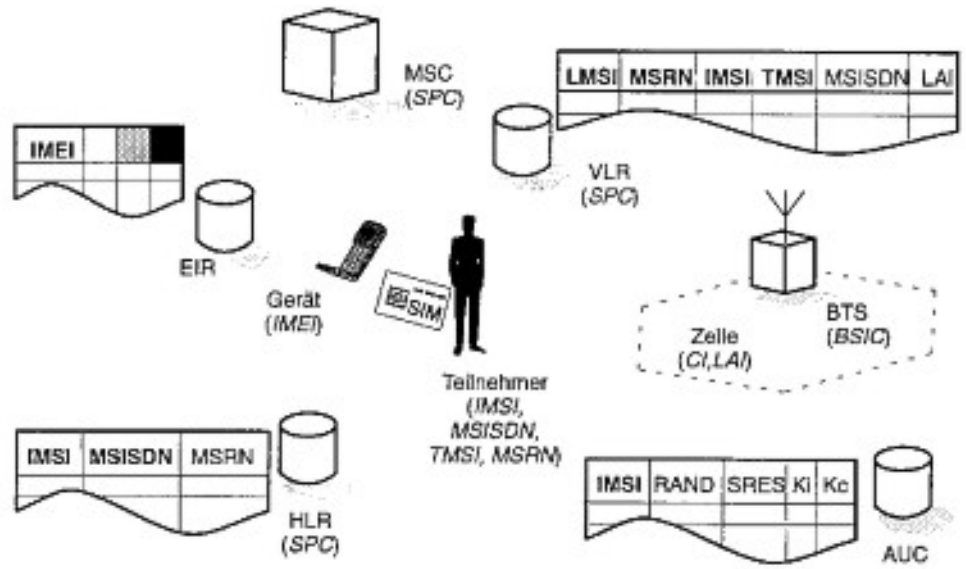


ABBILDUNG 21. Übersicht der Adressen und ihre zugehörigen Datenbanken

2.3.1 International Mobile Station Identity (IMEI)

Die IMEI kennzeichnet international eindeutig ein Mobilgeräte. Es ist eine Art Seriennummer. Sie wird vom Hersteller vergeben und den Netzbetreibern zu Verfügung gestellt, welche sie dann in Equipment Identity Registern (EIR) speichern. Mit der IMEI können veraltete, gestohlene oder nicht mehr funktionsfähige Geräte erkannt werden und beispielsweise vom Dienstzugang gesperrt werden. Dazu sind sie in drei Klassen unterteilt:

- white list alle Geräte
- black list gesperrte Geräte
- grey list fehlerhafte und veraltete Geräte

Die IMEI besteht aus folgenden Teilen:

- Type Approval Code TAC (6 Dezimalstellen), zentral vergeben
- Final Assembly Code FAC (2 Dezimalstellen), vom Hersteller vergeben
- Serial Number SNR (6 Dezimalstellen), vom Hersteller vergeben
- Spare SP (1 Dezimalstelle)

Eine IMEI=TAC+FAC+SNR+SP kennzeichnet also eindeutig ein Mobilgerät und lässt Rückschlüsse auf Hersteller und Produktionsdaten zu.

2.3.2 International Mobile Subscriber Identity (IMSI)

Jeder Teilnehmer erhält bei seiner Anmeldung eine eindeutige Kennziffer, die International Mobile Subscriber Identity IMSI zugewiesen. Diese IMSI wird in der SIM-Karte gespeichert. Eine Mobilstation kann nur mit einer SIM-Karte mit einer gültigen IMSI und gültiger IMEI im Gerät betrieben werden. Die IMSI wird beispielsweise zur richtigen Gebührenabrechnung verwendet.

Auch sie besteht aus mehreren Teilen:

- Mobile Country Code MCC (3 Dezimalstellen), international genormt
- Mobile Network Code MNC (2 Dezimalstellen), zur eindeutigen Kennzeichnung eines Mobilnetzes in einem Land
- Mobile Subscriber Identification Number MSIN (max. 10 Dezimalstellen), Nummer des Teilnehmers in seinem Mobilnetz.

Land	Netz	MCC	MNC
Schweiz	Swisscom	228	01
Schweiz	DiAx	228	02
Deutschland		262	
Frankreich		208	
Östereich		232	

TABELLE 10. Mobile Country Code verschiedener Länder

2.3.3 Temporary Mobile Subscriber Identity (TMSI)

Die Temporary Mobile Subscriber Identity (TMSI) wird dem Teilnehmer zeitweilig, vom für den Aufenthaltsort der MS zuständigen, VLR zugewiesen. Bei jedem wechsel einer LAI wird auch die TMSI gewechselt. Die TMSI ist dem HLR nicht bekannt, sie hat nur lokale Bedeutung. Die TMSI wird anstatt der IMSI zur eindeutigen Identifikation des Teilnehmers verwendet und dient dazu, dass der Teilnehmer seine IMSI nicht permanent über die Luftschnittstelle übertragen muss. Somit kann durch abhören der Funkkanäle kein Rückschluss auf die Teilnehmeridentität gezogen werden.
Die TMSI ist vollständig betreiberabhängig, wobei sie aus maximal 4 mal 8 bit bestehen darf und der Wert $FFFFFFFF_{hex}$ ausgeschlossen ist.

Die eindeutige Teilnehmeridentifikation erfolgt nun also über das Tupel (TMSI,LAI).

2.3.4 Mobile Subscriber ISDN Number (MSISDN)

Die Mobile Subscriber ISDN Number (MSISDN) ist die eigentliche Telefonnummer eines Mobilgerätes. Sie ist dem Teilnehmer zugeordnet und auf der SIM-Karte abgespeichert, so dass ein Gerät je nach SIM verschiedene MSISDN besitzen kann. Mit diesem Konzept der Trennung zwischen Teilnehmeridentität und Rufnummer ist es möglich, dass ein Teilnehmer mehreren MSISDN zugeordnet sein kann. Jede MSISDN ist dabei für einen entsprechenden Dienst reserviert (Sprache, Fax, Daten , etc.).
Die MSISDN richtet sich am internationalen ISDN-Nummerierungsplan und besitzt folgende Struktur:

- Country Code CC (bis 3 Dezimalstellen)
- National Destination Code NDC (typ. 2 bis 3 Dezimalstellen)
- Subscriber Number SN (max. 10 Dezimalstellen)

Die Länderkennziffern CC sind international nach ITU-T E.164 genormt. Eine MSISDN=CC+NDC+SN besitzt damit max. 15 Dezimalstellen. Sie wird zentral im HLR gespeichert.

CC der Schweiz:	041
NDC DiAX:	076
NDC Swisscom:	079

2.3.4.1 Mobile Station Roaming Number (MSRN)

Die Mobile Station Roaming Number MSRN ist eine temporäre, aufenthaltsabhängige ISDN-Nummer. Sie wird vom lokal zuständigen VLR jeder Mobilstation zugewiesen. Eine Kopie der MSRN wird im HLR gespeichert um Anrufe zu routeten.
Die MSRN besitzt den selben Aufbau wie die MSISDN.

2.3.5 Location Area Identity (LAI)

Jede Zelle (Location Area, LA) eines GSM-Netzes besitzt eine eigene Kennziffer. Die Location Area Identity (LAI) ist ebenfalls international eindeutig.
Sie besteht aus:

- Country Code CC (3 Dezimalstellen)
- Mobile Network Code MNC (2 Dezimalstellen)
- Location Area Code LAC (max. 5 Dezimalstellen oder 2 mal 8bit hexadezimal kodiert)

Die LAI wird von der Basisstation auf dem Broadcast Control Channel BCCH regelmässig ausgesendet. Mit der LAI ist es einem Mobilgerät jederzeit möglich seinen aktuellen Aufenthaltsort festzustellen. Wechselt das Mobilgerät von einer LAI zur anderen so stellt die MS den Wechsel der LA fest und fordert die Aktualisierung ihrer Aufenthaltsinformationen (Location Update) in den Registern HLR und VLR an. Die MS ist somit selbst dafür verantwortlich die aktuellen Empfangsbedingungen zu überwachen.
Mittels der LAI währe es nun also möglich Applikationen zu realisieren, die die Aufenthaltspossition auf „Zellengenauigkeit“ in eine Karte eintragen.

2.4 Funkschnittstellen

[1], [4]

2.4.1 Physikalische Kanäle und Multiplexierverfahren

Beim Funkkanal handelt es sich um ein von vielen Teilnehmern gemeinsam genutztes Übertragungsmedium. Die Mobilstationen der verschiedenen Teilnehmer konkurrieren um die Ressource Frequenz, um ihre Daten zu übertragen. Ohne eine zusätzliche Regelung des gleichzeitigen Zugriffs vieler Benutzer käme es zwangsläufig zu Kollisionen, was für eine verbindungsorientierte Kommunikation, wie der mobilen Telefonie, äusserst unerwünscht ist. Um dies zu verhindern werden spezielle Multiplexierverfahren eingesetzt.
Heute kommen vor allem drei Verfahren und Kombinationen davon zum Einsatz: Frequenz-, Zeit- und Codemultiplexierung. In GSM kommen allerdings nur Frequenz- und Zeitmultiplexierung zur Anwendung. Im weiteren wird in GSM auch ein Raummultiplexierungsverfahren zum Einsatz.

2.4.1.1 Frequency Division Multiple Access (FDMA)

Beim Frequency Division Multiple Access FDMA Verfahren wird das Frequenzband in gleich grosse Kanäle zerlegt, so dass Gesprächsverbindung auf unterschiedlichen Frequenzen geführt werden.

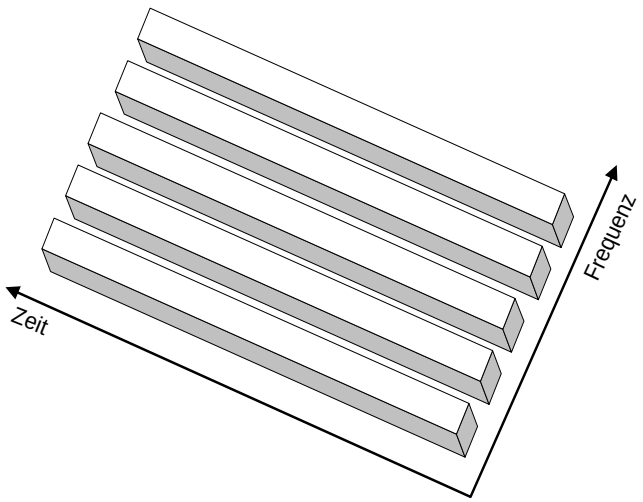


ABBILDUNG 22. Frequenz Division Multiple Access

2.4.1.2 Time Division Multiple Access (TDMA)

TDMA ist ein sehr aufwendiges Verfahren, da es eine hochgenaue Synchronisation zwischen Sender und Empfänger benötigt. Im GSM wird einer MS exklusiv für die Zeit eines TDMA-Zeitschlitzes eine Frequenz zugewiesen.

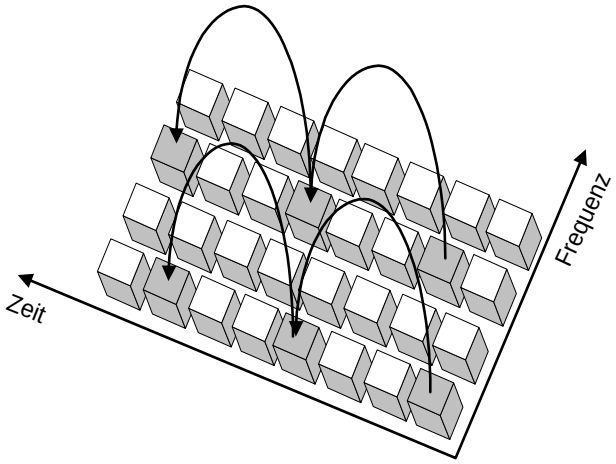


ABBILDUNG 23. Time Division Multiple Access

2.4.1.3 Anwendung im GSM

[4]

In GSM wird zwischen zwei Funkrichtungen unterschieden: Je nachdem, ob der Funkweg von der MS zur BSS, oder die umgekehrte Richtung gemeint ist, spricht man von Uplink bzw. Downlink.

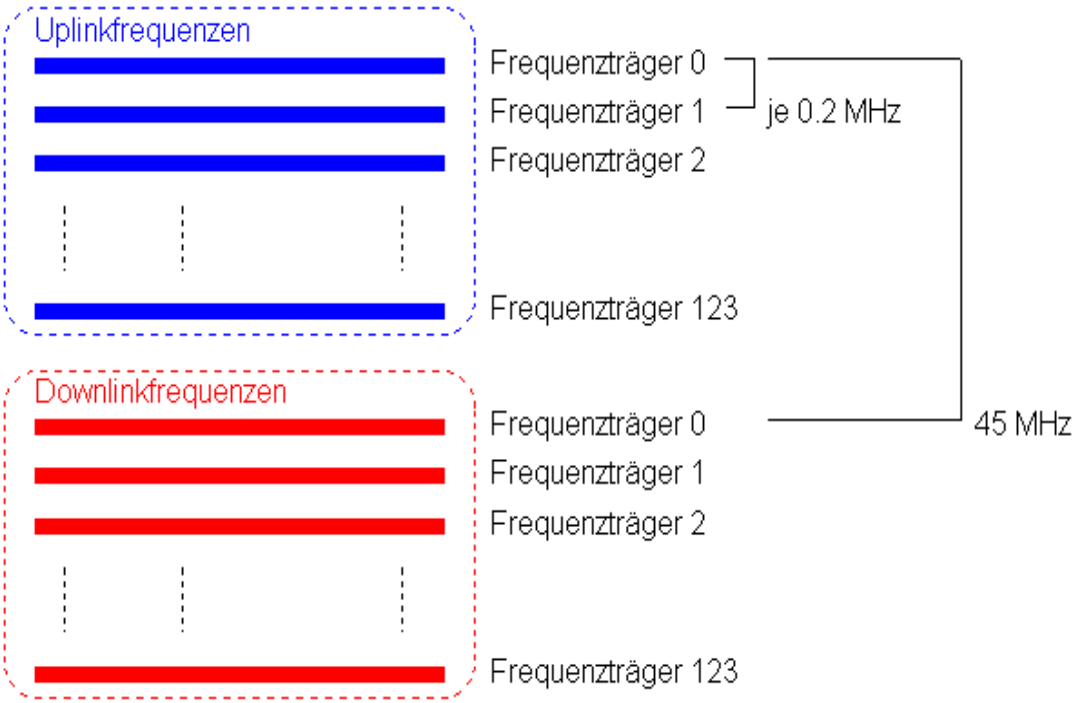
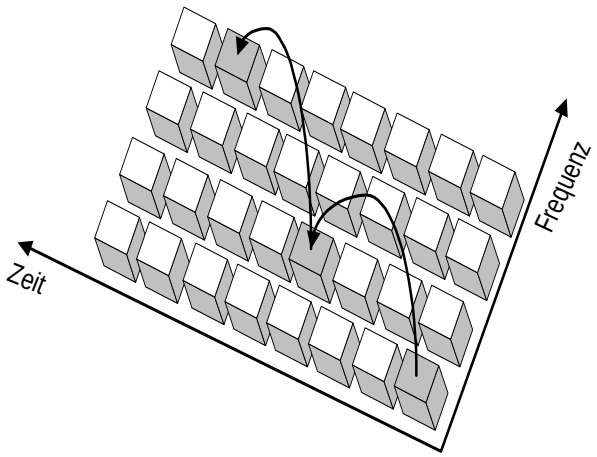


ABBILDUNG 24. Frequenzband Aufteilung

Jeder Funkkanal besteht aus einem solchen Uplink- und Downlinkpaar, wobei der Abstand der Up- und Downlinkfrequenz immer identisch ist (Duplexabstand) nämlich 45 MHz. Im GSM-Betrieb befindet sich der Uplinkbereich von 890 MHz – 915 MHz und der Downlinkbereich zwischen 935 MHz und 960 MHz (890 – 945=45). Jedes dieser Bänder von 25 MHz Breite (915-890=25) ist in 124 einzelne Kanäle mit 200 kHz Abstand unterteilt. Es bilden also immer zwei Bänder im Abstand von 45 MHz einen sogenannten Duplexkanal.

- f_{uplink}=890.2 MHz + (i-1) * 0.2 MHz
- $f_{downlink}$= f_{uplink} + 45 MHz
  (i =1..124)



Im weiteren kombiniert das GSM Sytem FDMA und TDMA in ein sogenanntes Mehrträger-TDMA-Vielfachzugriffsverfahren (Multi-Carrier-TDMA).

ABBILDUNG 25. TDMA -FDMA mitFrequenzsprungverfahre

Die oben beschriebenen Kanäle (aus FDMA hervorgehend) werden hierbei in acht TDMA-Gesprächskanäle unterteilt. Eine Folge von Zeitschlitzen, die eine MS zugewiesen bekommt, bildet den physikalischen Kanal eines TDMA Systems.

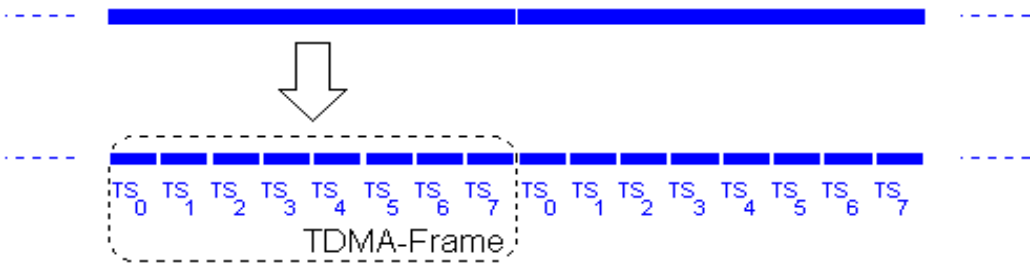


ABBILDUNG 26. TDMA-Frame

Eine Abfolge von acht Zeitschlitzen (time slots) heisst auch TDMA-Rahmen (auch Frame) und dauert 4,615 ms daraus folgt, dass ein Zeitschlitz 0,576875 ms dauert. Die pro Zeitschlitz übertragene Datenmenge wird als Date-Burst bezeichnet. Ein solcher Burst beinhaltet im Durchschnitt 156,25 bit (1 bit = 3,692 µs). Bei den hier beschriebenen Bursts handelt es sich also um Bitpakete. Die merkwürdig erscheinenden 0,25 bit sind bestandteil der Guard Period. Die Guard Period dient zum Schutz vor Überschwingern des Sendesignals beim Ein- bez. Ausschalten des Senders.

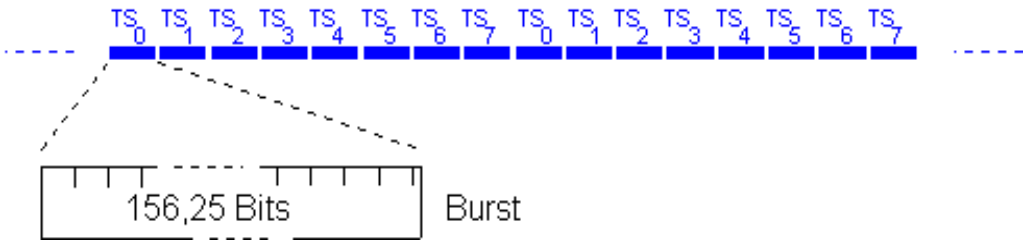


ABBILDUNG 27. Burst

2.4.1.3.1 Burst

Im GSM kennt man fünf Burstarten:

- Normal Burst, NB
  Der normal Burst wird verwendet um Informationen von Verkehrs- und Steuerkanälen zu übertragen. Die einzelnen Bursts sind durch 8,25 bit (Guard Period) getrennt. Am Anfang und am Ende des Burstabschnittes werden je 3 Tail Bits übertragen, die stets auf logisch “0” gesetzt werden. Sie füllen die Zeit aus während die Sendeleistung am Anfang und am Ende eines Bursts hoch bez. heruntergetastet wird. Darüber hinaus werden sie zur Demodulation benötigt. Ein normaler Burst enthält neben den Synchronisations- und Signalisierungsbit 2 mal 58 bit Fehlerschutzcodierte und verschlüsselte Nutzdaten, getrennt von der 26 bit langen Training Sequenz. Die Trainings Sequenz besteht aus einer bekannten vordefinierten Folge von Bitmustern , die zur Synchronisation verwendet werden.

- Frequenz Correction Burst, FB
  Dieser Burst wird zur Frequenzsynchronisation einer MS verwendet. Die ständig wiederholte Aussendung des FBs wird auch Frequency Correction Channel FCCH genannt. Die Datenbits wie auch die Tails sind beim FB auf logisch “0” gesetzt. Dies führt bei der GMSK Modulation, die bei GSM eingesetzt wird, dazu das ein unmodulierter Träger übertragen wird. Dieses Signal wird der Basisstation periodisch auf dem BCCH-Träger ausgestrahlt. Die MS kann sich also periodisch mit der Basisstation synchronisieren.

- Synchronization Burst, SB
  Der SB dient zur zeitlichen Synchronisation der MS mit der BTS. Neben einer langen Trainings Sequenz enthält er die laufende Nummmer des TDMA-Rahmens. Die wiederholte Ausstrahlung von SBs nennt man Synchronization Channel SCH.

- Dummy Burst, DB
  Der DM wird von der BTS ausgestrahlt wenn keine anderen Bursts zu versenden sind. Es handelt sich dabei um den selben Frequenz-Kanal auf dem der BCCH-Träger gesendet wird.

- Access Burst, AB
  Der AB besitzt eine wesentlich längere guard period und dient zum wahlfreien Zugriff auf den RACH.

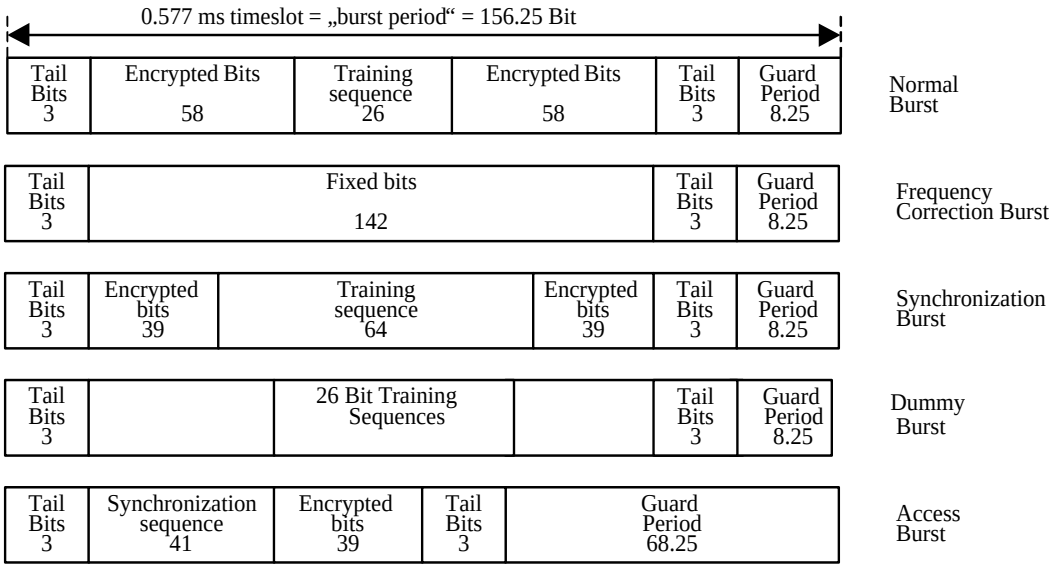


ABBILDUNG 28. Burst-Arten

2.4.2 Logische Kanäle

[4], [29]

GSM definiert eine Reihe von logischen Kanälen, die je nach Aufgabe, entweder im wahlfreien Vielfachzugriff (random access) oder bestimmten Benutzern zur Verfügung stehen.
Die logischen Kanäle werden in zwei Gruppen unterteilt:

- Verkehrskanäle, Traffic Channel TCH
  Sie werden zur Übertragung von Benutzerdaten (Fax, Daten, Sprache) genutzt. Sie transportieren keinerlei Signalisierungsinformationen. Die Kommunikation auf den TCH Kanälen kann paketvermittelt oder leitungsvermittelt geschehen. Für den paketvermittelten Modus der Nutzdaten stehen den X.25 Empfehlungen ähnliche standardisierte Paketprotokolle zur Verfügung. TCH Kanäle können im Full Rate (FTCH) oder Half Rate (HTCH) Betrieb genutzt werden.
- Signalisierungskanäle
  Die Signalisierungskanäle werden weiter in verschiedene Untergruppen unterteilt:
  - Broadcast Channel
    Sie sind unidirektional und senden immer an alle MS im Empfangsbereich einer BTS gleichzeitig.
    - Broadcast Control Channel, BCCH
    - Frequency Correction Channel, FCCH
    - Synchronization Channel, SCH
  - Common Control Channel, CCCH
    CCCH sind unidirektional und werden für die Funktionen des Zugriffsmanagements genutzt. Dazu gehört z.B. die Zuteilung von bestimmten Kanälen.
    - Random Access Channel, RACH

    - Access Grant Channel, AGCH
    - Paging Channel, PCH
- Dedicated/Associated Control Channel, DCCH/ACCH
    - Stand-alone Dedicated Control Channel, SDCCH
    - Slow Associated Control Channel, SACCH
    - Fast Associated Control Channel, FACCH

Die logischen Kanäle können nicht beliebig gleichzeitig genutzt werden. Sie können nur in bestimmten Kombinationen eingesetzt und auf physikalische Kanäle übertragen werden. In GSM sind sieben verschiedene Kanalkonfigurationen definiert worden, die von den BTS realisiert und angeboten werden. Eine Mobilstation kann also, abhängig von ihrem momentanen Zustand, nur auf eine Teilmenge der logischen Kanäle zugreifen.

2.5 Quellencodierung und Sprachcodierug

[4]

Die Quellcodierung reduziert die Redundanz im Sprachsignal, woraus sich eine Kompression des Signals ergibt, so dass eine deutlich geringere Bitrate zur Signalübertragung notwendig wird. Die Funktionen des GSM-Sprachcoders und –decoders sind meist in einem Baustein zusammengefasst, der CODEC genannt wird.
Senderseitig wird das Sprachsignal mit 8kHz Abtastfrequenz, nach dem auch hier gültigen Abtasttheorem, mit der zweifachen Signalbandbreite (menschliche Stimme ~4000Hz), abgetastet. Es wird eine Auflösung von 13bit *1)* verwendet, was zu einer Datenrate von 104kbit/s führt. Der Sprachcoder komprimiert nun dieses Signal mit einem Faktor 8, woraus sich eine Bitrate von 13kbit/s ergibt.

Zur Übertragung auf der Luftschnittstelle sind zwei Modi möglich:

- Kontinuierliche Übertragung
- DTX-Modus (Discontinous Transmission), d.h. 13kbit/s-Sprache werden nur dann übertragen, solange die VAD-Algorithmen (Voice Activity Detection) auch Sprache erkennen. Wird keine Sprache erkannt, werden alle 480 ms Daten zur Hintergrundgeräusch Nachbildung (comfort noise) in sogenannten SID-Frames (Silence Descriptor Frames) überragen.

Beim Zugang ins ISDN-Netz übernimmt die TRAU (Transcoder / Rate Adapter Unit) die Anpassung der Übertragungsrate an 64kbit/s ISDN. Es ist also so, dass das digitale, quellencodierte Sparchsignal der MS fehlerschutzcodiert und verschlüsselt über die Luftschnittstelle übertragen wird. In der BTS wird das Signal entschlüsselt und der Fehlerschutz vor der Weiterleitung entfernt. Diese auf dem Funkweg speziell gesicherte Sprachübertragung erfolgt transparent zwischen der MS und einer TRAU-Einheit, in der das GSM-kodierte Signal auf das Standard-ISDN-Format (nach ITU-T A) gewandelt wird. Für die Plazierung der TRAU stehen zwei Möglichkeiten zur Auswahl: die TRAU kann entweder in der BTS plaziert werden,

1) In der normalen Telefonie wird nur eine 8 bit Quantisierung vorgenommen. Hierbei ist aber zu beachten, dass es sich um eine nichtlineare Quantisierung handelt die mit einer linearen Quantisierung mit 12 bit zu vergleichen ist. Bei der in GSM verwendeten Quantisierung handelt es sich um eine lineare folglich ist sie nur um 1 bit genauer.

oder ausserhalb der BTS in der BSC. Sie sollte sich aber wenn möglich immer in der Nähe einer MSC befinden, um Übertragungskapazität auf den Verbindungsleitungen zu sparen.

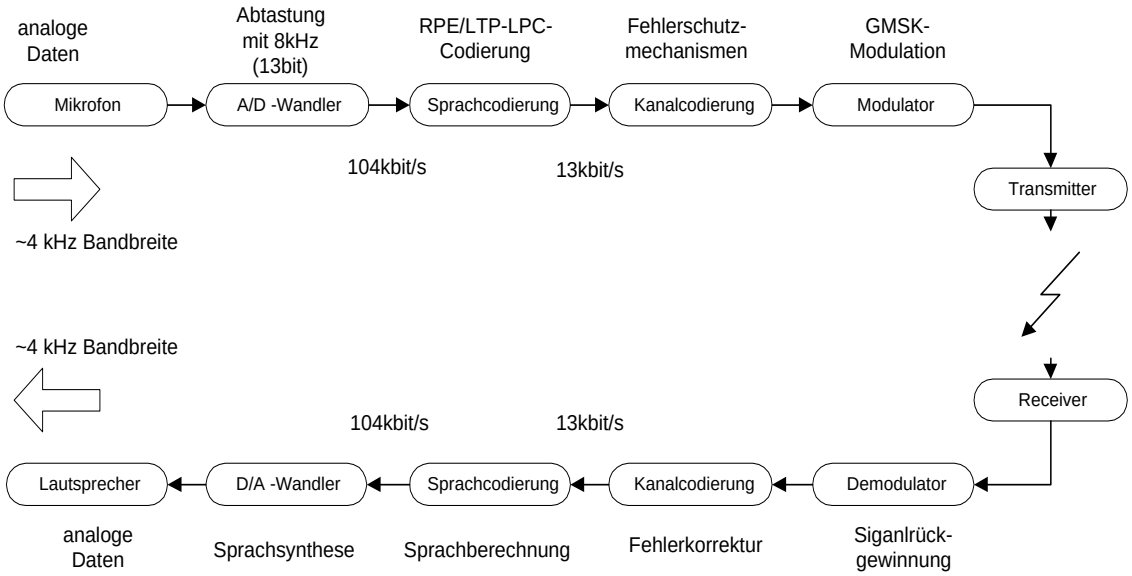


ABBILDUNG 29. Blockschaltbild Sprachcodierung

2.5.1 Sprachfunktionen Senderseite

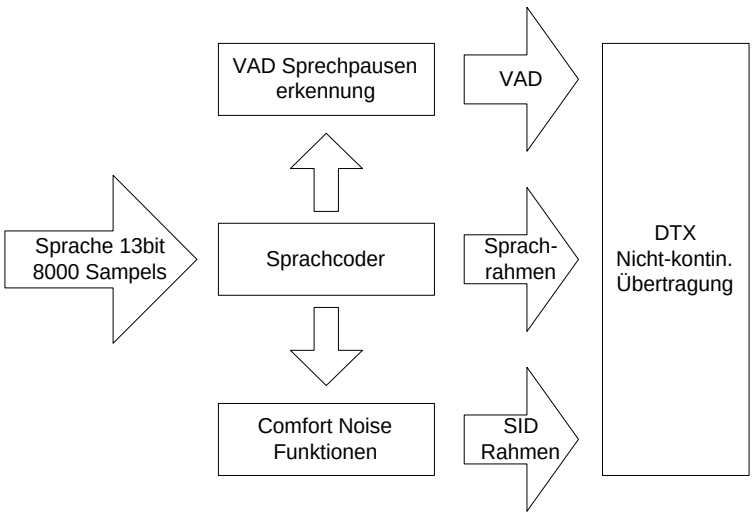


ABBILDUNG 30. Schema der Sprachfunktionen auf der Senderseite

- Sprachcoder
  Die eigentliche Srachkompression findet im Sprachcoder statt. In GSM wird ein Verfahren mit dem Namen Regular Pulse Excitation – Long Term Predication – Linear Predictive Coder kurz RPE/LTP-LPC (eine Abkürzung, für die man fast auch schon eine Abkürzung bräuchte...) angewendet.Da es sich bei diesem Verfahren um ein sehr komplexes und kompliziertes handelt wollen wir versuchen, es Anhand eines Beispiels, aus einem völlig anderem Bereich zu erklären: Angenommen, man wüsste das nur Klaviermusik übertragen würde. Dann genügte es, auf beiden Seiten ein Klavier (in Handyformat?...) vorzusehen; ein Algorithmus müsste dann “nur” die Noten und deren Spielweise senderseitig erkennen. Auf der Leitung würde dann nicht die Musik selbst übertragen, sondern nur noch abstraktere Information, wie "spiele einen Dominant-Sept-Akkord in c-moll" und einige zusätzliche Parameter.
  Nach einem ähnlichen Prinzip funktioniert das GSM-Verfahren auch, nur wird hier eben nicht Klaviermusik, sondern menschliche Sprache übertragen. Das heisst: das RPE/LTP-LPC-Verfahren ist in der Lage eine Modell von menschlicher Sprache zu erzeugen.

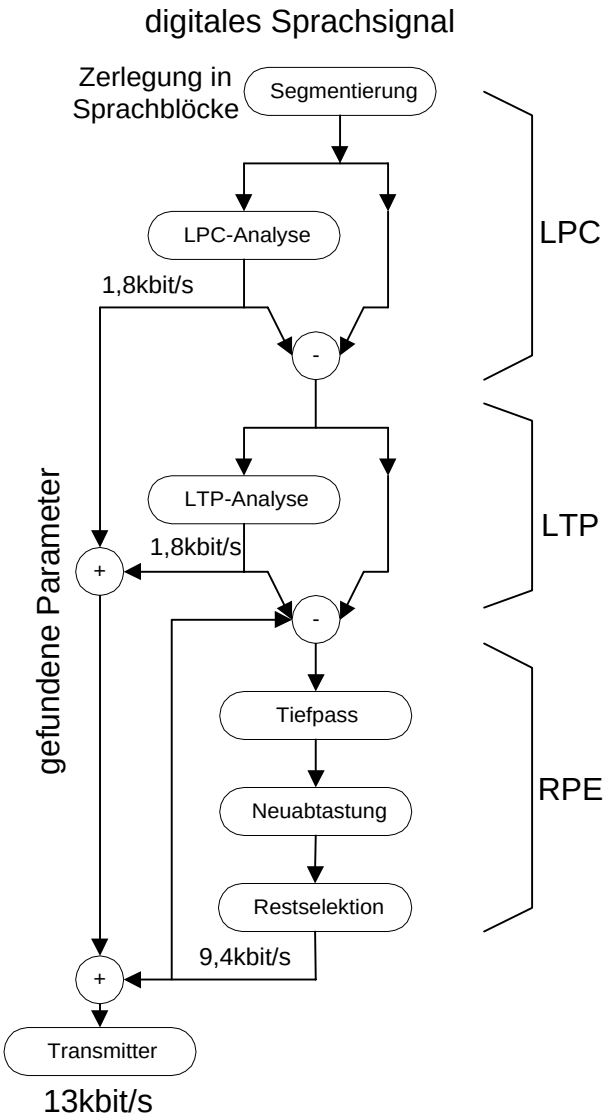


ABBILDUNG 31. Sprachcoder

Was geschieht nun in Wirklichkeit:

- LPC-Stufe
  Sie ist für die Übertragung der “Grobstruktur” des Signals verantwortlich. Die Sprache wird in 20ms-Happen zerlegt. In einer Art Codebuch wird nach möglichst passenden Anregungssignalen, Verstärkungs- und Filterparametern gesucht, die das Signal am besten synthetisieren können. Ein solcher Sprachblock kann erst bearbeitet werden, wenn er komplett vorliegt, was eine Verzögerung des Signals von mindestens 20ms zur Folge hat.

- LTP-Stufe
  Der “Langzeit-Predikations-Filter” berücksichtigt hauptsächlich längerdauernde statische Abhängigkeiten der menschlichen Sprache (z.B. Silben) und kann daher in der menschlichen Stimme auftretende periodische Signalanteile effektiv erfassen. Auch diese Teil generiert also eine Anzahl von Parametern die zur Wiederherstellung des Signals benötigt werden.

  - RPE-Stufe
    Das Signal hat nun eine deutlich reduzierte Dynamik (flaches Amplitudenspektrum). Anders gesagt, die wichtigsten Teile des Sprachsignals sind schon durch die anderen Stufen erfasst worden. Die Aufgabe der RPE-Stufe ist es nun, subjektive, irrelevante Sprachinformationen des Restsignals wegzulassen.

- Voice Activity Detection, VAD
  Der Sprechpausen-Detektor entscheidet aufgrund verschiedener Parameter ob es sich beim vorliegenden Sprachramen um Sprache oder eine Sprachpause handelt. Diese Entscheidung dient zur Abschaltung des Sendeverstärkers bei Sprechpausen.

- Discontinous Transmission, DTX
  Die DTX nutzt die Tatsache, das während eines Gesprächs meist nur einer spricht während der Andere zuhört. In jeder Übertragungsrichtung müssen also nur etwa zur Hälfte der Gesprächsdauer Sprachdaten übertragen werden. Durch die Aktivierung des DTX-Modes wird die Sendeleistung verringert und so die Akkulebensdauer vergrössert.

- Comfort Noise, CN
  Fehlerhafte Sprachrahmen werden empfangsseitig durch ein synthetisches Hintergrundgeräusch ersetzt. Die Parameter für den Comfort-Noise-Synthesizer werden in einem SID-Rahmen übertragen.

- Silence Descriptor, SID
  Das SID wird Senderseitig durch dauernde Messung des Hintergrundgeräusches generiert. DAS SID ist ein Sprachrahmen der am Ende eines Sprachbursts, also am Anfang einer Sprachpause, übertragen wird. Der Empfangsseite kann also das Ende eines Sprachbursts signalisiert werden und der Comfort-Noise-Synthesizer erhält die nötigen Parameter zur Aktivierung. Durch das so künstlich generierte Hintergrundgeräusch wird verhindert, dass man während einer Sprachpause von einer “digitalen Stille” irritiert wird, was vom menschlichen Gehör als äusserst störend empfunden würde.

2.5.2 Sprachfunktionen Empfängerseite

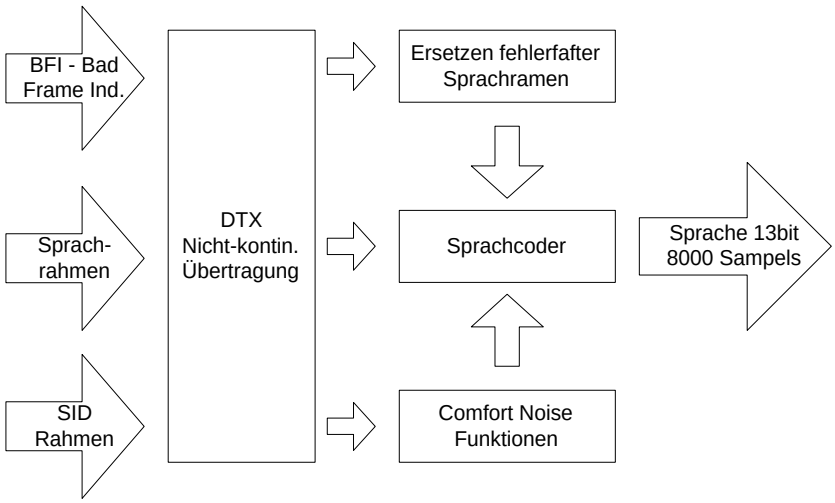


ABBILDUNG 32. Schema der Sprachfunktionen auf der Empfängerseite

- Bad Frame Indication, BFI
  Sind Sprachrahmen aufgrund von Übertragungsfehlern nicht mehr verwendbar, werden sie auf der Empfangsseite vom Kanalcoder mit einem BFI-Flag signalisiert. In diesem Fall wird der Sprachrahmen verworfen und dieser betroffene Rahmen durch einen berechneten (aproximierten) ersetzt. Diese Technik wird als Fehlerverdeckung (error concealment) bezeichnet. Werden mehr als 16 Rahmen hintereinander verworfen, wird der Empfänger auf stummgeschaltet, um den temporären Ausfall des Kanals zu signalisieren.

Die hier nicht erwähnten Komponenten des Empfangsteiles entsprechen in weiten Teilen denen im Sendeteil.

2.6 Datenübertragung

[4]

Im GSM Standard sind Teletext, Videotext und Gruppe-3-Fax-Dienste spezifiziert worden. Da GSM speziell für die Sprachübertragung optimierte Codieralgorithmen verwendet, lassen sich diese nicht so leicht verwenden wie im öffentlichen Telefonnetz. Für eine reine GSM zu GSM Übertragung müssen keine Tonmodems verwendet werden, da es sich um ein rein digitales Netz handelt. Da durch Abschattung und Störungen die Übertragung auf dem Funkweg kurzzeitig gestört sein kann, sind spezielle Fehlerbehandlungen notwendig.
Es sind verschiedene Zugänge zu den öffentlichen Datennetzen möglich. Es wird zwischen transparenten (9.6 kbit/s – 2.4 kbit/s) und nicht transparenten Trägerdiensten unterschieden.
Der GSM Standard bietet auch ein Punkt-zu-Punkt Paging Service (Short Message Service, SMS), der ohne zusätzliche Geräte (Notebooks,...) auskommt.

Das grösste Problem der Datenübertragung über den Funkweg ist die hohe Fehlerrate (bis 10^{-3}). Aus diesem Grund werden verstärkte Fehlersicherungsverfahren notwendig. Im transparenten Übertragungsmodus werden Nutzdaten von 9600 bit/s unterstützt.
Im nicht transparenten paketorientierten Modus wird das RLP-Protokoll (Radio Link Protokoll) verwendet. Fehlerhafte Rahmen (Frames) werden wiederholt. Dieser Modus ist nicht transparent, da er den Protokoll-Overhead anderer Protokolle (z.B. X.25) wie Synchronisation, Informationen zur Datenrate des eigenen Protokolls umwandelt und so 9600 bit/s Nutzdatenrate ermöglicht.

- Frage:
  Warum kann der digitale 13 kbit/s Kanal eines GSM-Systems nicht unmittelbar zur Datenübertragung, z.B. mit einem Modem, benutzt werden?

  Antwort:
  Am Eingang und Ausgang des 13 kbit/s –Kanals befindet sich ein Coder/Decoder, der auf die statischen Eigenschaften des Sprachsignals abgestimmt ist. Das Sprachsignal hat im unteren Drittel des Bandes von 300-3400 Hz seine grösste Leistungsdichte, das Datensignal jedoch im oberen Bereich. Daraus ergeben sich unterschiedliche Anforderungen für die Kanalcodierung/ Modulation.

2.7 Fehlerschutzmechanismen

[1], [4]

Da bei der Datenübertragung per Funk die Bitfehlerhäufigkeit sehr hoch ist wird beim GSM-System ein erheblicher Aufwand zur Sicherung der Daten gegen Übertragungsfehler betrieben. Zum einen wird dazu die gerade eben erst durch die Sprachcodierung mühsam verringerte Bandbreite durch Hinzufügen von Redundanz und Prüfsummen wieder auf 22.8kbit/s erhöht, zum anderen werden aber auch raffinierte Übertragungstricks angewendet.

- Redundanzerhöhung:
  Im GSM-System werden die Daten, wie bereits erwähnt, in 20ms-Blöcken übertragen. Bei einer Nutzdatenrate von 13kbps entspricht dies also zunächst 260 Bit (13kbps * 1s/20ms) grossen Datenpaketen.
  Diese werden nun schrittweise auf 456 Bits ergänzt (=22.8kbps):
  - Umordnen
    Die Daten werden gemäss ihrer Wichtigkeit in 3 Klassen aufgeteilt:
    - 50 sehr wichtige Bits
    - 132 wichtige Bits
    - 78 wenige wichtige Bits

  - Prüfsumme
    Für die als wichtigsten eingestuften Bits wird eine CRC-Summe (3 Bit) berechnet
    50 Bit + 3 Bit = 53 Bit

  - Erweiterung und erneute Umordnung
    An die “wichtigen” Klassen, Klasse1 und Klasse2, werden nun insgesammt 4 sogenannte Tailbits “0000” angehängt. Diese auf den ersten Blick unsinnige Massnahme erhöht nochmals den Schutz von Bits am Anfang und Ende der (53+132) Bitsequenz, so dass eine erneute Umordnung vorgenommen wird, bei der die wichtigsten Bits an den Rand dieses 185 Bitblocks versetzt werden.
    ((53 Bit + 132 Bit) + 4 Nullbit) = 189 Bit

  - Faltung
    Die vorderen Bitblöcke mit den insgesamt 189 als "wichtig" klassifizierten Bits werden nun einem sogenannten “Faltungscodierer” unterzogen, der den Datenumfang letztlich durch Einfügung von Redundanz verdoppelt.
    2 * 189 Bit = 378 Bit

    Nach dem Falzungscodierer werden nun noch die als wenig wichtig eingestuften Bit angehängt.
    378 Bit + 78 Bit = 456 Bit

Der Verwendete Faltungscodierer ist dabei ein relativ einfach aufgebauter Baustein:

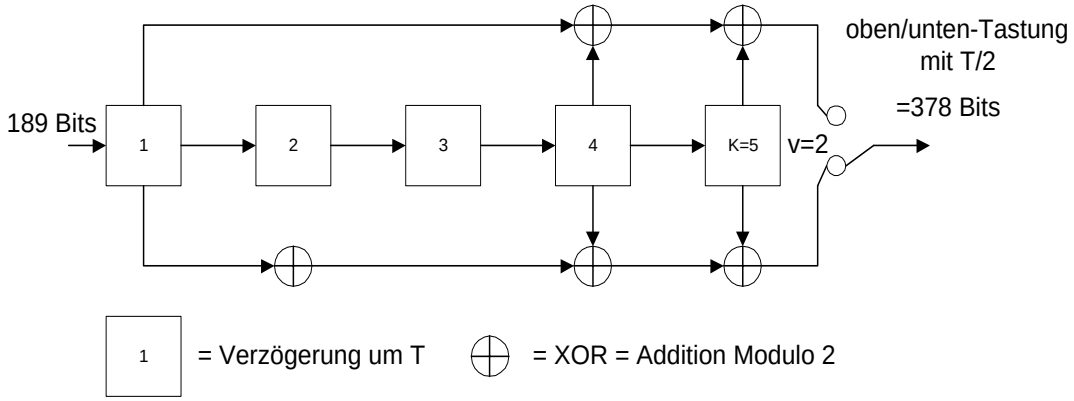


ABBILDUNG 33. Faltungscodierer

Dieses Verfahren erlaubt im Mittel die Korrektur von ~25% aller Übertragungsfehler.

- Übetragungstricks
  Da vielmals verschiedene Arten von Übertragungsfehlern gemeinsam auftreten, d.h. sowohl zeitlich als auch frequenzmässig, versucht das GSM-System, die zu übertragenden Daten über die Zeit und die Frequenz zu streuen, um die Auswirkungen von Blockfehlern so abzumildern, dass sie durch die Redundanz wieder korrigiert werden können.
  - Bit-Interleaving
    Das Bit-Interleaving ("Verspreizung") verteilt die 456 Bits eines Sprachblocks über 8 Datenpakete, um Fehler über die Zeit (=mehrere Rahmen) zu streuen. Zusätzlich werden ursprünglich benachbarte Bits möglichst weit über die 8 Datenpakete verstreut, um somit auch die Zerstörung benachbarter Bits zu vermindern.
    (Für die GSM-Datendienste wird das Verfahren noch weiter getrieben: Hier werden die Bits auf bis zu 19 Pakete verteilt; das ist bei den Sprachdiensten jedoch nicht möglich, denn das empfängerseitige Zusammenklauben der verteilten Informationen bedeutet längere Wartezeiten, bis der Datenblock vorliegt und die so resultierende Verzögerung wäre für interaktive Sprache zu lang).
  - Frequency-Hopping
    Zusätzlich werden die Informationen auch über das Frequenzspektrum gestreut, d.h. die einzelnen Datenpakete werden auf verschiedenen Trägerfrequenzen verschickt, so dass die Störung einer Frequenz weniger ins Gewicht fällt.
  - Extrapolation
    Wenn all dies nichts nützt, dann kann sich das System auf der Empfangsseite noch mit einem aus der CD-Technik bekannten Trick aushelfen:
    Ist das empfangene Datenpaket nicht wiederherstellbar, so wird es schlicht ignoriert und statt dessen der Parametersatz des letzten Sprachrahmens verwendet. Technisch bewirkt dies eine Interpolation der Ausgangswerte, die subjektiv kaum bemerkbar ist. Erst nach 320ms kontinuierlich falschen Sprachrahmen wird der Ausgang komplett stumm geschaltet.

2.8 GMSK Modulation

[4]

Im GSM System wird zur Modulation auf dem Funkkanal das Gauss Minimum Shift Keying (GMSK) verwendet. GSMK gehört zur Familie der kontinuierlichen Phasenmodulationsverfahren. Besondere Vorteile dieses Verfahrens sind einerseits die schmalen Senderleistungsspektren und andererseits die konstanten Hüllkurven, die es erlauben in den Sendern besonders einfache Verstärker, ohne besondere Linearitätsanforderungen, zu verwenden. Die Verstärker sind besonders kostengünstig und besitzen einen hohen Wirkungsgrad, was einen geringen Verbrauch und lange Betriebszeiten bei akku-betriebenen Geräten ermöglicht.

Bei digitalen Modulationsverfahren für die GSM-Luftschnittstelle sind mehrere Schritte zu unterscheiden.

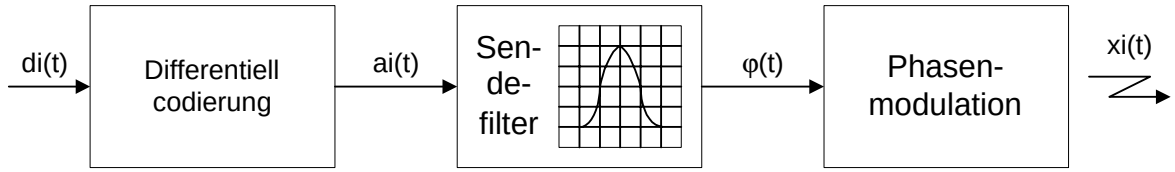


ABBILDUNG 34. Stufen der Kanalkodireung

- Differenzielle codierung
  Das Resultat der differenzielle Codierung ist eine Folge von Dirac-Impulsen. Sendefilter
  Die Impulsantwort des Gauss-Tiefpassfilters wird durch die Faltung einer Rechteckfunktion mit der Impulsantwort eines Gauss-Tiefpasses beschrieben
  .

$$g(t) = h(t) * rect(t/T)$$

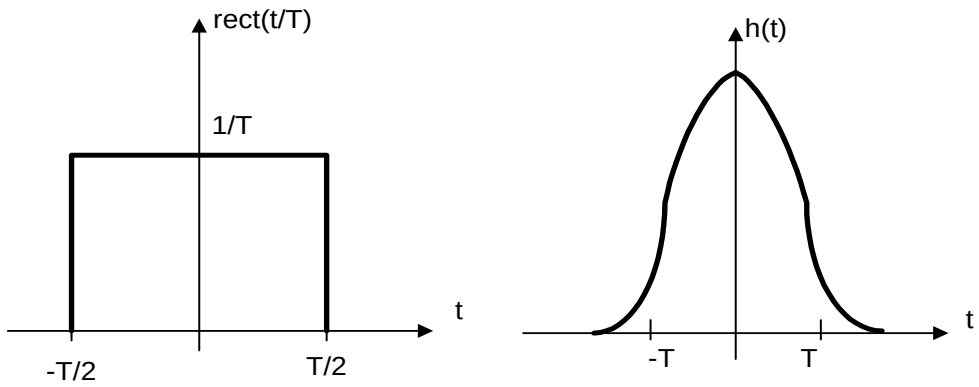


ABBILDUNG 35. Impulsantwort des GMSK-Sendefilters

Die Gauss-Tiefpassfilterung der Rechteckfunktion bewirkt eine zusätzliche Glättung, aber auch eine Verbreiterung der Impulsantwort g(t), was eine Verschmälerung des Leistungsdichtspektrums des Signals zur Folge hat.

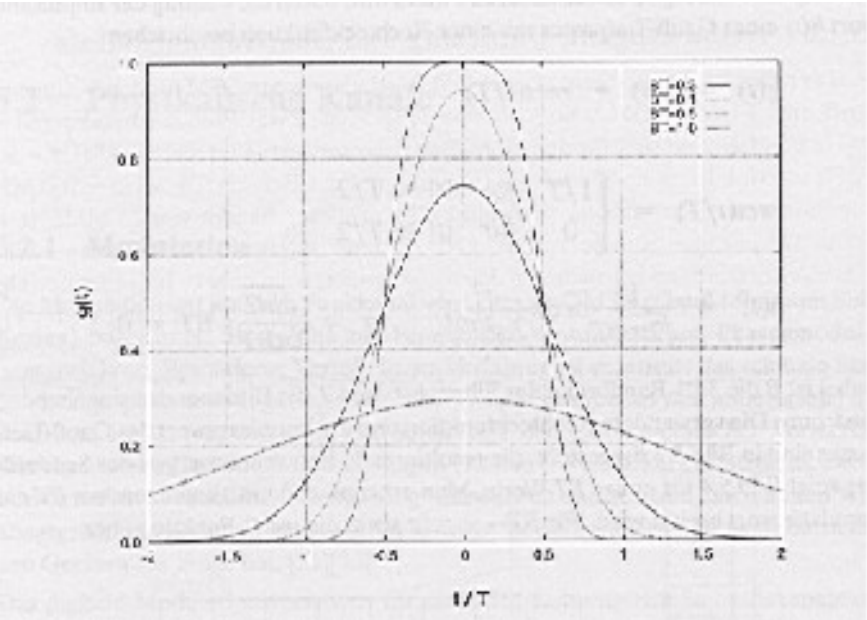


ABBILDUNG 36. Reale Impulsantwort des Gauss-Tiefpasses

- Die Phase φ(t) des Modulationssignals ist die Faltung der Impulsantwort g(t) des Sendefilters mit der Dirac-Impulsfolge des Modulationsdatenstroms.

  Der Modulationsindex η ist ½ , d.h. die maximale Phasenänderung (Phasenshift) beträgt $\pi/2$ je Bitintervall.

- Schliesslich wird die Phase φ(t) nun auf einen Phasenmodulator gegeben um das modulierte HF-Trägersignal x(t) zu erhalten.

2.9 Sicherheitsaspekte

[1],[4], [29]

Methoden zur Datenverschlüsselung gewinnen in modernen digitalen Systemen enorm an Bedeutung. Entsprechend wurden im GSM leistungsfähige Algorithmen und Verschlüsselungstechniken implementiert.
Es werden folgende Dienste unterschieden:

- Subscriber Identity Authentication
  (Nachweis der Teilnehmeridentität)
- Data Confidentiality for Physical Connections
  (Vertraulichkeit der physikalisch übertragenen Daten)
- Subscriber Identity Confidentiality
  (Vertraulichkeit der Teilnehmeridentität)
- Signalling Information Element Confidentiality
  (Vertraulichkeit von Informationselementen der Signalisierungsprozeduren auf dem Funkweg)

2.9.1 Schutz der Teilnehmeridentität

Hiermit soll ausgeschlossen werden, dass durch Abhören des Signalisierungsverkehrs auf dem Funkkanal festgestellt werden kann, welcher Teilnehmer welche Ressourcen im Netz benutzt. Damit soll die Lokalisierung und Verfolgung einer MS verhindert werden. Das heisst vor allem, dass die IMEI normalerweise nicht im Klartext übermittelt werden darf.

Die IMSI wird nur über den Funkkanal übertragen, wenn der MS noch keine TMSI zugewiesen wurde. Ist eine MS dann im lokalen VLR registriert und besitzt eine TMSI wird nur noch sie zur Teilnehmeridentifikation auf dem Funkkanal verwendet. Zusätzlich wird auch die TMSI nur verschlüsselt übertragen. Da die TMSI temporär ist kann ein Teilnehmer nur in Verbindung mit der LAI eindeutig identifiziert werden. Die Zuweisung TMSI-IMSI geschieht im VLR, welches die TMSI auch an die MS vergibt.

2.9.2 Verifizierung der Teilnehmeridentität

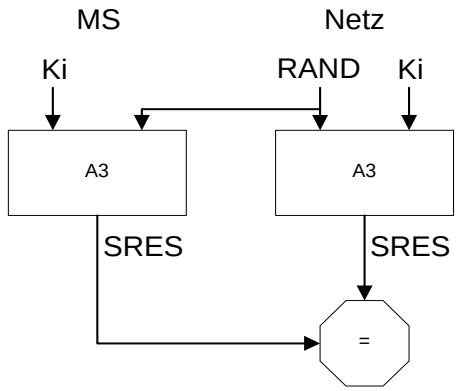


ABBILDUNG 37. Verifizierung der Teilnehmeridentität

In der Authentifikation-Prozedur wir geprüft, ob eine SIM-Karte, und somit ihr Besitzer, berechtigt ist in ein GSM-Netz einzusteigen und so dort zu telefonieren. Die ganze Authentifikation basiert auf einem A3-Algorithmus, der in der SIM-Karte und im Netz gespeichert ist. Der Algorithmus benutzt einen Schlüssel, den Ki, der im AuC des Heimnetzes und in der SIM-Karte abgelegt ist. Zusätzlich wird eine Zufallszahl RAND benötigt, die zur MS übertragen wird. Mittels des A3-Algorithmus wird dann SRES generiert und dann ins AUC zurückgesendet. Im AuC wird gleichzeitig auch das SRES generiert und dann mit dem SRES der MS verglichen. Sind sie identisch wird der Netzzutritt gewährt.
Ein wichtiger Sicherheitsfaktor ist, dass der Ki und der A3-Algorithmus nie über Funk übertragen werden.

2.9.3 Verschlüsselung von Signalisierungs- und Nutzdaten

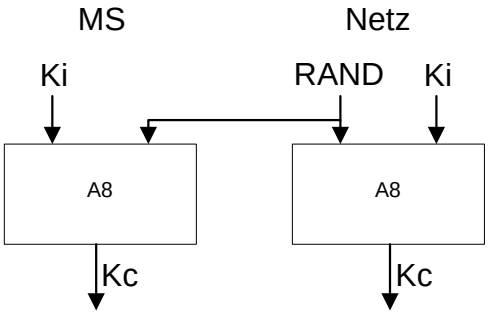


ABBILDUNG 38. Kc generierung

Um die übermittelten Daten zu verschlüsseln und entschlüsseln, wird ein A5-Algorithmus verwendet. Damit die Sicherheit gewährleistet wird, wird zusätzlich ein Schlüssel Kc generiert, der vom A5-Algorithmus genützt wird. Der A8-Algorithmus generiert mit Hilfe des Ki und RAND diesen Kc Schlüssel. Der A8-Algorithmus ist in der SIM-Karte und im Netz abgelegt.

Die Chiffrierung von Signalisierungs- und Nutzdaten erfolgt in der MS und in der BTS. Es handelt sich dabei um ein symmetrisches Kryptoverfahren, d.h. Chiffrierung und Dechiffrierung werden mit dem gleichen Schlüssel Kc und dem A5-Algorithmus durchgeführt.

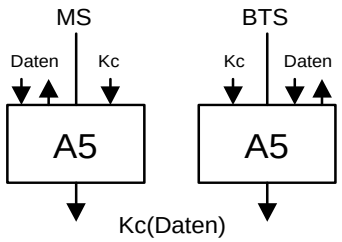


ABBILDUNG 39. Datenchiffrierung

Verknüpfung von Nutzdatenstrom und Schlüsselstrom erfolgt mittels einer EXKLUSIVE-ODER-Verknüpfung.

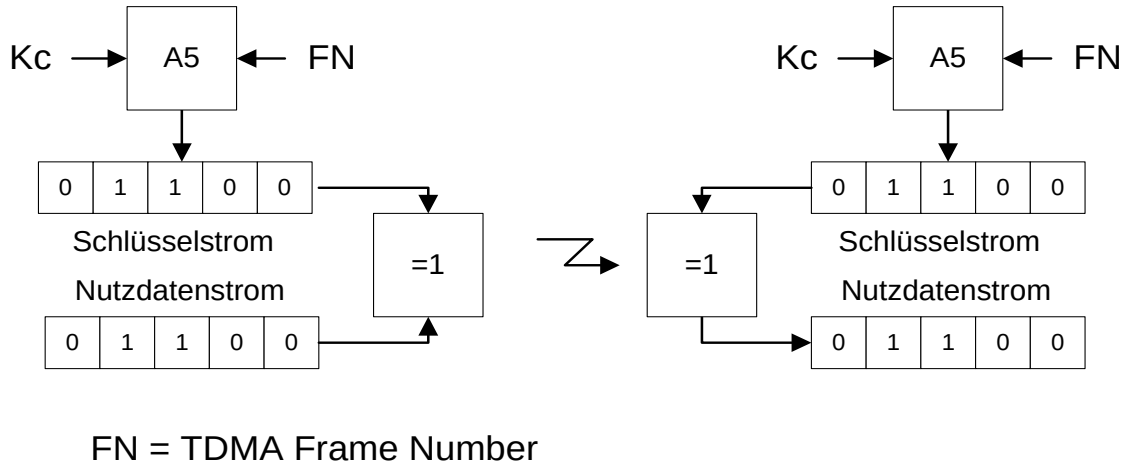


ABBILDUNG 40. Datenverschlüsselung

2.10 Roaming

[27]

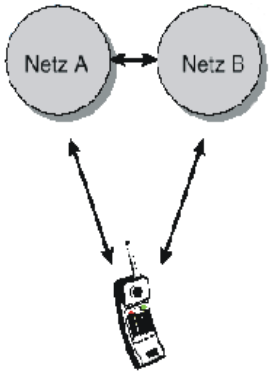


ABBILDUNG 41. Roaming

Mit Roaming wird der Übergang eines Teilnehmers in ein Fremdnetz bezeichnet. Es werden also unterschiedliche Netze mit einem Endgerät benutzt, dies setzt den gleichen Netztyp voraus.
Damit man z.B. mit einem Swisscom Abonnement in Deutschland telefonieren kann, sind sogennante Roamingverträge zwischen den Netzanbietern nötig. In diesen Roamingverträgen sind verschiedene Dinge unteranderem die Kostenfrage bei der benutzung des Fremdnetzes geregelt.

2.10.1 SIM-Roaming

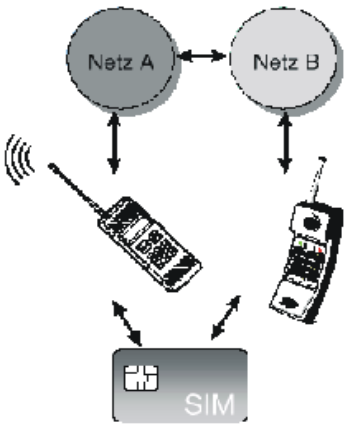


ABBILDUNG 42. SIM-Roaming

Hier kommt wieder die strickte Teilung zwischen Gerät und Teilnehmer zum Zuge. Über die genormte Schnittstelle zwischen ME und SIM wird es einem Teilnehmer ermöglicht seine SIM-Karte in ein beliebiges Endgerät einzusetzen, um sich so ins lokale Netz einzuwählen. Man nimmt also nur die SIM-Karte mit. Wirkungsvoll ist das SIM-Roaming z.B. beim Übergang in Netze der USA, da in den USA sich die Trägerfrequenzen des GSM bei 1900 MHz befinden und nicht wie in Europa bei 900 MHz und 1800 MHz und dadurch MS auch nicht für den Gebrauch in diesen Frequenzbereichen ausgelegt sind. Selbstverständlich muss dazu zwischen den Netzberteibern in Europa und den USA das Interworking implementiert sein, damit das Zusammenspiel HLT / VLR funktioniert. Bei diesen Vereinbarungen handelt es sich um die oben erwähnten Roamingverträge. Hierbei ist zu beachten, dass die Funktion des VLR im fremden Netz liegt, das eventuell mit anderer Technik aufgebaut wurde.

Da der Übergang vom 900 MHz ins 1800 MHz bez. 1900 MHz Netz also mit einer normalen MS nicht möglich ist, da die Endgeräte in unterschiedlichen Frequenzbereichen arbeiten. Wurden sogennante Dualband Endgerät entwickelt, die in verschiedenen Frequenzbereichen einsetzbar sind. Diese Dualband Endgeräte gibt es in verschieden Frequenzkombinationen (900-1800 MHz, 900-1900 MHz).

2.11 Handover

[4], [27]

Handover kann zwischen zwei Zellen (Intercell Handover) oder zwischen zwei Kanälen (Intracell Handover) erfolgen. Verschiedene Gründe können zu einem Handover führen:

- Bewegung des Teilnehmers
- Hohe Verkehrslasten
- Wartungsmassnahmen (im Netz)
- Messung des Funkfeldes durch die MS (Signalstärke)

Die BSS entscheidet, über welche BTS eine MS angesprochen werden soll, anhand der Kriterien:

- Empfangsfeldstärke
- Kanalqualität
- Augenblickliche Verkehrslast der Zelle
- Verfügbarkeit von BTS (z.B. bei Wartungsarbeiten)

Man unterscheidet zwei Arten von Handover

- Intra-Cell-Handover:
  Aus administrativen Gründen oder auch wegen der Kanalqualität erhält eine MS innerhalb einer Zelle einen neuen Kanal zugewiesen. Der Entscheid wird lokal von der BSS getroffen und durchgeführt.
- Inter-Cell-Handover:
  Die Verbindung einer MS wird über eine Zellgrenze hinweg einer neuen BTS zugewiesen. Die Entscheidung über den Zeitpunkt des Handovers wird aufgrund von Messdaten der MS und des BSS getroffen. Meist erfolgt ein Inter-Cell-Handover dann, wenn eine hohe Bitfehlerhäufigkeit, aufgrund schwacher Empfangsfeldstärke und schlechter Kanalqualität, festgestellt wird. Dies ist meist dann der Fall, wenn sich die MS am Rande einer Zelle befindet.

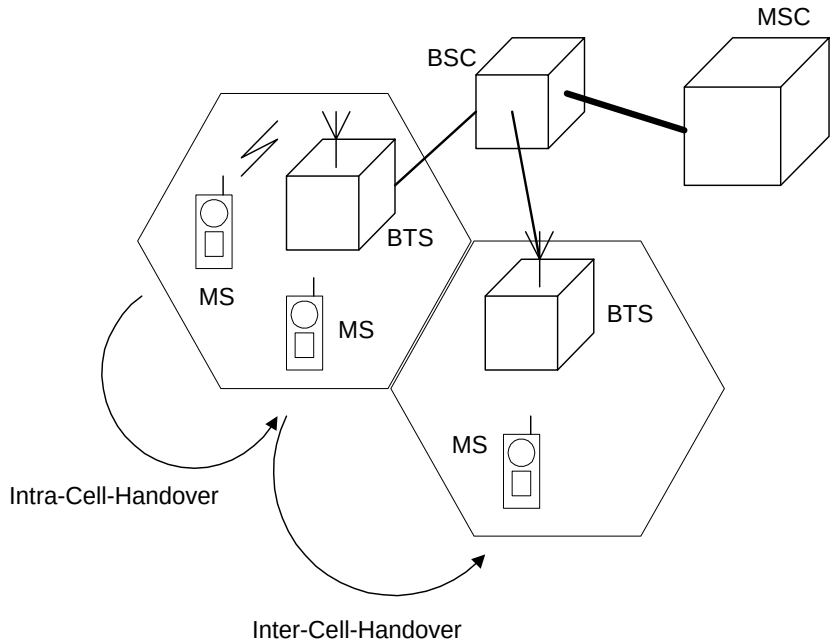


ABBILDUNG 43. Handover

2.12 Short Message Service (SMS)

[6]

2.12.1 SMS-Point-to-Point-Service

[1], [7]

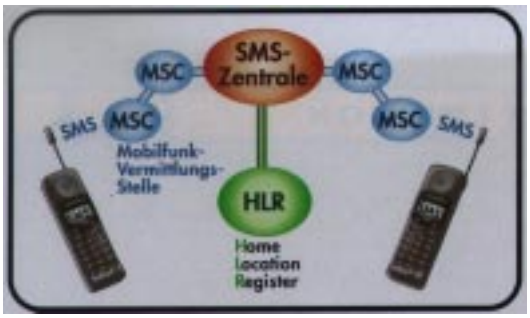


ABBILDUNG 44. Short Message Service

Geht eine SMS-Nachricht vom Mobiltelefon ab, teilt das Funktelefon der Basisstation mit, wohin sie den SMS-Datenblock senden soll. Die Übermittlung von Kurznachrichten erfolgt mit einem verbindungslosen, paketvermittelnden Protokol. Per SMS ist es möglich, mit einer Mobilstation eine bis zu 160 alphanumerische Zeichen lange Nachricht zu versenden. Adresse der Daten ist dabei nicht die Rufnummer des Empfängers, sondern die im Handy eingetragene SMS-Zentralnummer. Die einzelnen Mobilfunk-Vermittlungsstellen senden die Kurznachricht zur SMS Zentrale (Service Center, SC). Die SMS Zentrale ist ein Dienstzentrum, welches nach dem Store-and-Forward-Prinzip arbeitet. Geht die Kurznachricht von dort an ein Handy weiter, muss die SMS-Zentrale zunächst feststellen, wo sich das Empfängertelefon befindet. Dazu stimmt es sich mit dem Home-Location-Register des eigenen Mobilfunknetzes ab. Ist dort bekannt, wo das Empfänger-Handy zu finden ist, kann die SMS-Nachricht ordungsgemäss an die für das Empfänger-Handy zuständige Mobilfunk-Vermittlungsstelle weitergeleitet werden. Der Empfang einer Nachricht muss von der Mobilstation, bzw. dem Service Center, quittiert werden. Die Übertragung von Kurznachrichten ist gesichert. Treten während der Übertragung einer Nachricht Störungen auf, wird sie wiederholt. Allerdings gibt es keine Rückmeldung darüber, wann bzw. ob überhaupt eine Nachricht auch gelesen wurde. Es ist aber noch zu erwähnen, das eine SMS-Nachricht nur für eine bestimmte Zeit in der SMS Zentrale gespeichert wird. Wird die SMS-Nachricht während diese Zeit nicht an das Empfänger-Handy übermittelt, da es Beispielsweise ausgeschaltet ist, wird sie gelöscht.

2.12.1.1 SMS Datenpakete

[6]

Beim SMS-Point-to-Point-Service werden zwei Betriebsarte, abhängig vom Empfänger, unterschieden:

- Short Message Mobile Terminated Point-to-Point (SM MT)
  SM MT ermöglicht die Übertragung einer SMS vom der SMS Zentrale (Service Center, SC) zur MS.
- Short Message Mobile Originated Point-to-Point (SM MO)
  SM MO ermöglicht das versenden von SMS von Handys an SMS-Empfänger, wie z.B. ein MS oder ein SC, über ein SC. Die versendete SMS muss die Adresse des Empfängers beinhalten.

Der Short Message Transfer Layer (SM-TL) stellt 6 verschiedene Short Message Transfer Protocol Data Units (SMS-TPUD) zur verfügung um die oben genannten Betriebsarten zu realisieren.

- SMS-Deliver
  Übermittelt eine SMS-Nachricht vom SC zu einer MS

- SMS-Deliver-Report
  Bestätigung der Übertragung oder Fehlermeldungen bei SMS-Deliver.
- SMS-Submit
  Übermittelt eine SMS-Nachricht von einer MS zum SC.
- SMS-Submit-Report
  Bestätigung der Übertragung oder Fehlermeldungen bei SMS-Submit.
- SMS-Status-Report
  Beinhaltet Informationen darüber ob es dem SC z.B. möglich war das SMS weiterzuleiten oder ob es zwischen gespeichert wurde.
- SMS-Command
  Über dieses TPUD ist es einem MS z.B. möglich eine im SC gespeicherte SMS zu löschen oder einen SMS-Status-Report anzufordern.

2.12.1.2 SMS Frame

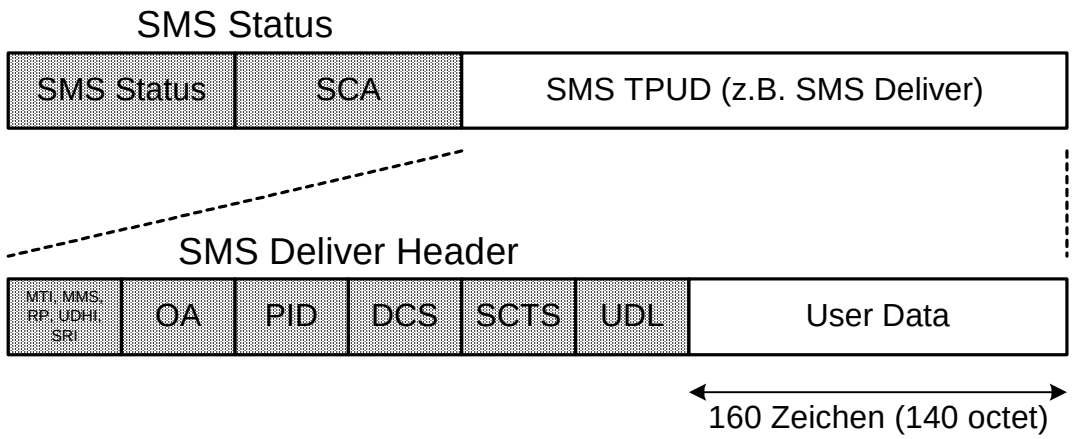


ABBILDUNG 45. SMS Frame

Der Aufbau des SMS Frames wird hier anhand der Protocol Data Unit (PUD) SMS Deliver genauer betrachtet.

2.12.1.2.1 SMS Header Format

Der SMS Heder beinhaltet Daten die für alle SMS-Nachrichten-Formate benötigt werden.

Anzahl Bytes	Beschreibung
1	SMS Status (wird unten genauer beschrieben)
2 bis 12	Service-Center-Adress (SCA) (wird unten genauer beschrieben)

TABELLE 11. SMS Header Format

- SMS Status Feld

[8]

b7	b6	b5	b4	b3	b2	b1	b0	Beschreibung
0	0	0	0		x	x	x	SMS Status
					0	0	0	Freier platz
					0	0	1	Durch MS erhaltene Nachricht - gelesen
					0	1	1	Durch MS erhaltene Nachricht - nicht gelesen
					1	0	1	Von MS abgehende Nachricht - gesendet
					1	1	1	Von MS abgehende Nachricht - nicht gesendet

TABELLE 12. SMS Status Feld

- SCA Feld

[7]

Anzahl Bytes	Beschreibung
1	Adress länge (beinhaltet Adresswert und TON/NPI)
1	Type of Numbre / Numbering Plan Identification (TON/NPI) *1)*
1 bis 10	Adresswert

TABELLE 13. Service-Center-Adress Feld

1) TON/NPI sind in GSM 04.08 genau spezifiziert

2.12.1.2.2 SMS Deliver TPUD Header Forma

[6]t

Abk.	Name	P *1)*	R *2)*	Beschreibung
TP-MTI	TP-Message-Type-Identicator	M	2b	Nachrichtentype
TP-MMS	TP-More_Message-to-Send	M	b	Zeigt an ob noch Nachrichten folgen
TP-RP	TP-Replay-Path	M	b	Zeigt an ob ein Replay-Path mitgesendet wird
TP-UDHI	TP-User-Data-Header-Indicator	O	b	Zeigt an on der TP-UD einen Header beinhaltet
TP-SRI	TP-Status-Report-Indicator	O	b	Zeigt an ob ein Status Report gefordert wird
TP-OA	TP-Originating-Adress	M	2o - 12o	Adresse des Empfängers
TP-PID	TP-Protocol-Identifier	M	o	Parameter für Übergeordnete Layer
TP-DCS	TP-Data-Coding-Scheme	M	o	Art der Codierung der Daten im TP-UD
TP-SCTS	TP-Service-Center-Time-Stamp	M	7o	Zeitpunkt indem das SC die Nachricht empfing
TP-UDL	TP-User-Data-Length	M	I	Länge von TP-UD
TP-UD	TP-User-Data	O	*3)*	Benutzerdaten

TABELLE 14. SMS Deliver TPUD Header Format

1) Provision; Mandatory (M) oder Optional (O)

2) Representation; Integer (I), bit (b), 2 bits (2b), Octet (0), 7 Oczets (7o), 2-12 Octets (2o - 12o)

3) Von TP-DCS abhängig

2.12.2 Cell Broadcast Service

[4]

Eine weitere Variante der Kurznachrichtendienste ist der Cell Broadcast Service (Short Message Service Cell Broadcast SMSCB, TS23) . Die SMSCB-Nachrichten werden in einem begrenzten, regionalen Teil eines Netzes ausgestrahlt. Sie können von Mobilstationen nur im Ruhezustand (Idle-Mode, es wird kein Gespräch geführt) empfangen werden, und der Empfang wird nicht quittiert. Eine Mobilstation kann keine SMSCB-Nachrichten senden. Bei diesem Dienst erhalten die Kurznachrichten nach Kategorien eine eindeutige Kennzeichnung, so daß eine Mobilstation gezielt nur die sie interessierenden Kategorien von Nachrichten ernpfangen und speichern kann. Die maximale Länge einer SMSCB-Nachricht sind 93 Zeichen, wobei allerdings mit einem speziellen Verkettungsmechanismus längere Nachrichten, bestehend aus bis zu 15 aufeinanderfolgenden SMSCBs, versendet werden können.

3.0 Subscriber Identity Module (SIM)

[18]

ABBILDUNG 46. Smartcard

Die SIM ist eine Smartcard, welche einen Prozessor, RAM, ROM und ein EEPROM integriert hat. Sie ist auf einer Karte mit der Grösse einer Kreditkarte integriert. Da diese Karte für einige Mobiltelefone zu gross ist, gibt es eine kleinere Version der SIM, die nur die Grösse des Chips hat (plug-in SIM). Ohne die SIM Karte funktioniert das Mobiltelefon nicht. Auf der SIM Karte sind Parameter des Benutzers gespeichert. Zusätzlich werden persönliche Daten, die vom Abonnenten benutzt werden können gespeichert (z.B. Telefonnummern). Mittels SIM wird der Abonnent auf dem Netzwerk identifiziert. Da die persönlichen Daten nur auf der SIM gespeichert sind, kann man im Ausland seine SIM Karte in einem gemietetem Telefon benutzen (SIM-Roaming). Man hätte die selbe Nummer wie zu Hause und alle Anrufe würden dem persönlichen Konto belastet.

Im EEPROM werden der GSM Algorithmus für die Authentifikation und Codierung, SMS Nachrichten und ein PIN (Personal Identification Number) gespeichert. Um die SIM Karte vor Missbrauch zu schützen, muss vor dem Gebrauch der Mobilstation ein 4-Stelliger PIN eingegeben werden. Falls der PIN 3 mal hintereinander falsch eingegeben wird, wird die Karte gesperrt, und kann nur mit einem 8-Stelligem PUK (Personal Unblocking Key) wieder zum laufen gebracht werden.

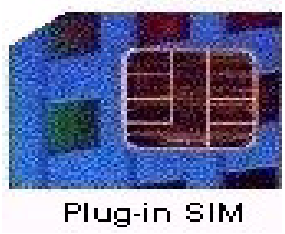


ABBILDUNG 47. Plug-in SIM

3.1 SIM Architektur

[20]

Die SIM-Karten benutzen den internationalen anerkannten Standard für Chipkarten mit Kontaktfeld, nämlich die ISO/IEC-Normen 7816-1 bis –4. Das Handy initialisiert die Kommunikation mit der SIM-Karte- “Master-Slave”-Prinzip. Der Datenaustausch zwischen SIM-Karte und ME läuft asynchron im Halfduplexverfahren ab. Das Taktsignal versorgt lediglich den integrierten Mikroprozessor. Alle Aspekte der Kommunikation zwischen ME und SIM-Karte sind in ISO 7816-3, ISO 7816-4 und ETSI GSM 11.11 geregelt. Die Syntax der Kommandos an die SIM und die resultierenden Empfangsbestätigungen an das ME, sogenannte APDUs (Application Data Protocol Units), sind in ETSI GSM 11.11 festgelegt.

- Gebräuchliche Kommandos sind z.B:
  - **SELECT FILE** Auswahl eines Datenbereiches
  - **READ BINARY** Daten lesen
  - **UPDATE BINARY** Daten schreiben
  - **VERIFY PIN** Vergleich einer PIN-Nummer mit der Referenz in der Chipkarte
  - **SEEK** String in File wird gesucht
  - **RUN GSM ALGORITHM** wird benutzt um Authentifikationsschlüssel Kc zu berechnen

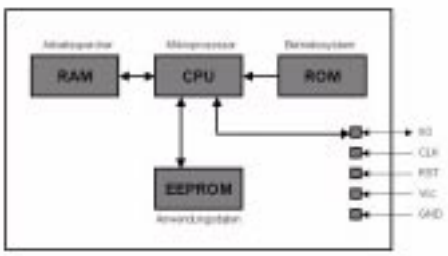


ABBILDUNG 48. Blockschaltbild SIM-Karte

- **File Struktur**
  Die Stuktur der Files in der SIM-Karte wird in vier Directorystufen unterteilt. Es werden vier verschiedene Typen von Files angewandt:
  - transparent files, um Daten zu speichern, die nicht formatiert sind (z.B. Schlüssel)
  - linear fixed files um formatierte Daten zu speichern (z.B. Telefonnummern)
  - cyclic files um formatierte Daten in chronologischer Reihenfolge zu speichern (z.B. akkumulierte Gesprächszähler)
  - script files um neue Karten Applikationen zu speichern

- **File Organisation**
  Das Betriebssystem der Karten organisiert die Files in einer hierarchischer Baum-struktur. Es werden drei verschiedene Arten von Files gehandelt:
  - Master Files (MF)
  - Dedicated Files (DF): enthält Elementary Files (EF) aber keine Daten
  - Elementary Files (EF): Ein File welches Daten enthält.

Eine SIM-Karte muss ein MF beinhalten (level 0). Die DF‘s (level 1, 2 und 3) sind optional.

ABBILDUNG 49. Filestruktur SIM-Karte

- **Master Files (MF)**
  - Kann Dedicated Files (DF) und Elementary Files (EF) beinhalten. Verwaltet den EEPROM-Speicher.
  - Enthält EF mit PIN1, PIN2, ADM1 und ADM2
    - Pin1:
      - Muss eingegeben werden, um Handy benutzen zu können
      - Muss in GemXplore eingegeben werden, um Files zu lesen
    - Pin 2
      - Wurde von uns nie benötigt
    - ADM1
      - Wird benötigt, um Programme auf die Karte zu laden
      - Wird benötigt, um Files zu erstellen
      - Wird benötigt, um Verzeichnisse in Verzeichnissen zu erstellen
    - ADM4
      - Wird benötigt, um Verseichnise im Master File zu erstellen
      - Wird benötigt, um Files und Verzeichnisse zu löschen

- **Dedicated Files (DF)**
  Das 1. Level beinhaltet verschiedene DF Files. Unter anderem $DF_{TELECOM}$(7F 10h) und DF_{GSM}(7F20h).

  $DF_{TELECOM}$(7F 10h) beinhaltet unter anderem EF mit folgenden Daten:
  - Emfangene SMS (pro Nachricht werden 176 bytes Speicherplatz benötigt)
  - Persönliche Telefonnummern mit Namen (1 Name mit 10 Buchstaben und Tel.Nr. benötigt ca. 26 bytes Speicherplatz)
  - MSISDN

  DF_{GSM}(7F20h) beinhaltet Informationen über das GSM-Netzwerk. Unter anderem EF mit folgenden Daten:
  - Kc
  - Phasenidentifikation der Karte (Phase 1,2 oder 2+)

- **Spezielle Files für SIM Toolkit Applikationen**
  Phase 2+ SIM Karten enthalten spezielle Files für SIM Toolkit Applikationen. Eine Applikation wird in einem eigenen DF abgespeichert. Es sind noch andere EF Files auf der Karte vorhanden:
  - EF_{AAC}: gibt an, ob andere Files im gleichen DF gelesen oder beschrieben werden dürfen.
  - EF_{MENU}: gibt die Adresse des DF an, in welchem die Applikation gespeichert ist
  - $EF_{Card\ Menu\ Title}$: Titel der Applikation

3.2 Entwicklung der SIM

Seitdem die SIM vor 10 Jahren konzipiert wurde, sind ihre funktionalen Anforderungen immer wieder erweitert worden. Die Karte wurde ursprünglich als Sicherheitsmodul für die Benutzerauthentifikation mit zusätzlichem Speicher für Benutzerdaten wie z.B. Telefonnummern und Netzwerkinformationen entwickelt. Das sind heute immer noch ihre Hauptaufgaben. In den verschiedenen GSM-Phasen wurde ihr EEPROM Speicher von ca. 1KB auf 16 KB erhöht.
Durch die vollständige Nutzung des Mikroprozessors hat die SIM die Fähigkeiten um die Plattform für Zusatzdienste darzustellen. Um diese Dienste SIM + ME unabhängig nutzen zu können, begann man 1994 Standards für SIM data-download over the air (Datenübertragung in die SIM über die Luftschnittstelle) und proactive SIM (ein Mechanismus welches der SIM erlaubt, Befehle an das ME zu schicken) festzulegen. Diese zwei Funktionen bilden die Basis eines neuen Standards, das SIM Application Toolkit. SIM Toolkit definiert zusätzlich zu ETSI 11.11 (SIM-ME interface) Befehle, um unabhängig vom ME Applikationen auf der SIM auszuführen.

Weltweite Kartenhersteller:

- Gemplus (wird durch Swisscom und diAx benutzt)
- Setec
- DeLaRue
- Schlumberger
- Philips
- ORGA

Diese Hersteller bieten verschiedene Karten mit unterschiedlichem EEPROM Speicher an:

Setec

Bezeichnung	GSM Phase	EEPROM Speicher	ROM	RAM
GSM SIM	2	8 KB	13- 15 KB	240-256 bytes

TABELLE 15. Setec SIM-Karten

DeLaRue

Bezeichnung	GSM Phase	Speicher	Speisespannung
SIM1	1	1 KB	5V
SIM2	2	8 KB	5V
SIM 3	2	8 KB	3-5V
SIM 4	2	16 KB	3-5V

TABELLE 16. DeLaRue SIM-Karten

GEMPLUS

Bezeichnung	GSM Phase	Speicher	Speisespannung
GemXplore 3K	2	3 KB	5V
GemXplore 4K	2	4 KB	3V + 5V

TABELLE 17. GemPlus SIM-Karten

GemXplore 8K	2	8KB	3V + 5V
GemXplore 16 K	2	16Kb	3V + 5V
GemXplore 98	2 +	16 KB	3V +5V

TABELLE 17. GemPlus SIM-Karten

Schlumberger

Bezeichnung	GSM Phase	Speicher	Speisespannung
SIMflex	2	1 KB	3-5 V
SIMflex	2	3 KB	3-5 V
SIMflex	2	8 KB	3-5 V
SIMflex	2	16 KB	3-5 V
Activa	2 +	16 KB	3-5 V

TABELLE 18. Schlumberger SIM-Karten

Orga

Bezeichnung	GSM Phase	EEPROM Speicher	ROM
SIMtelligence	2	16 KB	20 KB
SIMtelligence	2 +	16 KB	35 KB

TABELLE 19. Orga SIM-Karten

3.3 Natel Easy SIM-Karten

[32]

Neben den “normalen” SIM-Karten, bei denen eine monatliche Grundgebühr bezahlt werden muss, gibt es die sogenannten “Prepaid SIM Cards”. In der Schweiz sind sie als Natel-EASY bekannt. Im Gegensatz zu den fixen monatlichen Basisdienstpreisen bezahlt man bei den EASY-Karten nur soviel, wie man effektiv telefoniert. Dafür wird auf NATEL-Verbindungen ein Zuschlag für abgehende und ankommende Gespräche erhoben. Anruf und Empfang von ausländischen Telefonaten ist auch möglich.Gespräche auf Telekiosk- und Telebuisness-Nummern (156/157), sowie auf bestimmte Dienstnummern sind aber nicht möglich. Seit Anfang dieses Jahres ist es auch möglich, SMS zu senden und empfangen. Das Ausfüllen eines Vertrages entfällt.
Das Gesprächsguthaben kann jederzeit auf dem Mobiltelefon abgerufen werden. Falls kein Gesprächsguthaben mehr auf der Karte vorhanden ist, kann die Karte nachgeladen werden. Dazu gibt es 2 verschiedene Möglichkeiten:

- Es kann eine Value-Card gekauft werden, auf der sich ein Rubelfeld befindet, welches eine Sicherheitsnummer ab deckt. Diese Nummer kann über eine spezielle Zugangsnummer via Tastatur eingegeben werden. Innerhalb einer Stunde wird der Taxwert auf der Karte erhöht.
- Ein bestimmter Betrag kann über einen Einzahlungsschein einbezahlt wrden. Der einbezahlte Betrag wird innerhalb von etwa einer Woche gutgeschrieben.

NATEL easy funktioniert nur mit Mobiltelefonen, welche “Advice of Charging”*1)* (AOCC) und Short Message Service Mobile Terminated (SM MT) unterstützt.

Unter http://www.swisscom.com/gd/products/mobile_phones/natel_easy_ok_no_set-de.html sind die Mobiltelefone aufgeführt, welche diese technischen Anforderungen erfüllen.

1) Advice of Charging: Gebührenanzeige, wird von Mobiltelefone ab Phase 2 unterstützt

3.3.1 Funktionsweise

[24], [25]

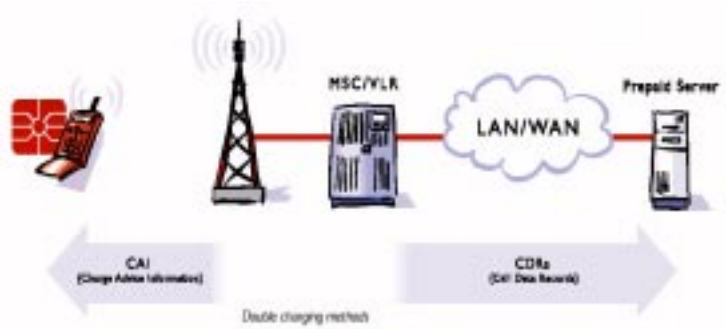


ABBILDUNG 50. Natel-Easy Funktionsweise

Natel Easy ist ein System welches von der Swisscom entwickelt wurde. Da wir keine genaueren technischen Angaben zum System fanden, haben wir das System von AU Systems beschrieben, welches auch auf Prepaid Karten basiert. Der Mechanismus, der dazu dient, die SIM Karte mit der Telefongebühr zu belasten, basiert auf den zwei ETSI Phase 2 Diensten AOCC und Charge Advice Information *2)* (CAI). Alle Mobilitelefone ab Phase 2 unterstützen diese Dienste. Die Kommunikation zwischen Prepaid Server und Mobiltelefon geschieht mit Hilfe der SMS-SC mittels SMS. Sobald jemand, der eine Prepaid SIM Karte benutzt, sich ins Netzwerk einloggt, erkennt das MSC dass eine Prepaid SIM Karte benutzt wird. Sie sendet Tarifinformationen an die Karte und den Prepaid Server. Die Telefongebühr wird auf der Karte abgezogen. Zusätzlich werden die Daten auf dem Prepaid Server in den Call Data Records (CDRs) gespeichert. Falls das Gesprächsguthaben aufgebraucht ist, kann der Server die Karte automatisch deaktivierten. Durch diese doppelte Kontoführung (auf der Karte und auf dem Prepaid Server) ist die Sicherheit gewährleistet. Falls auf einer SIM Karte aus irgend einem Grund ein Fehlbetrag ist, kann mittels Prepaid Server der Betrag in den CDR auf die Karte geladen werden.

2) Gebührenzählung

4.0 Services

Die Zahl und Vielfalt der angebotenen GSM-Services wird von Tag zu Tag grösser. Auch werden sie seitens des Anbieters immer aufwendiger und komplexer. Ob es sich um nötige oder sogar sinnvolle Dienste handelt sei dahingestellt. Wir haben versucht die uns bekannten Services in fünf Kategorien zu unterteilen.

- Geschäftlich
- News
- Auskunftsdienste
- Gateway
- Freizeit

4.1 Geschäftlich

- Kaufangebote bzw. Kaufgesuche
- Finanzinformationen (FinPhone)
  - Devisenkurse
  - Aktienkurse

  Beispiel: Sendet man das Schlüsseltwort ABBN an die Zielnimmer 305 so wird einem der momentane Wert der ABB-Namenaktie zugestellt.
  http://www.swisscom.ch/gd/services/mobile_com/natel/telekurs-de.html
- Kommunikation mit Aussendiensten
- Terminbestätigungen
- Postphone
  Mit Postphone haben Sie jederzeit die Möglichkeit den Stand Ihres Gelben Kontos über Ihr Handy abzufragen.
  So funktioniert's:
  Sie senden die folgende Kurzmeldung an die Kurznummer >800<: POSTPHONE, Sprachcode, Postkontonummer, Code der Abfrageart, PIN-Code.
  Die Eingabe erfolgt immer ohne Leerschlag nach dem Komma. Voraussetzung ist, dass Sie über einen eigenen PIN-Code verfügen. Machen Sie den Versuch mit folgender Meldung auf dem Testkonto:
  Saldoabfrage: POSTPHONE,D,2597798,1,123456 und senden an Nummer >800<.
  Abfrage der letzten Buchungen: POSTPHONE,D,2597798,2,123456 und senden an Nummer >800<.
  http://www.swisscom.ch/gd/services/mobile_com/natel/postphone_detail-de.html

In diesem Gebiet liegt meiner Meinung nach ein grosses Potential, es wird wohl auch am schnellsten erweitert werden.

4.2 News

- Sportnachrichten
  Dies umfasst Ergebnisse jeglicher Art wie Halbzeitstände, Tabellen, Weltranglisten, Rennergebnisse, Endresultate oder spezielle Ereignisse aus :
  - Fussball
  - Fussball WM 98
  - Tour de France 98
  - Formel 1
  - Tennis
  - Golf
  - Eishockey (z.B Ergebnisse EV Zug von Minick)
  - Die neuesten Nachrichten
  - Wetter

  http://www.swisscom.ch/gd/services/mobile_com/natel/sayings-de.html

4.3 Auskunftsdienste

- Abfragen von Telefonnummern
  Sie haben eine Rufnummer auf ihrem Handy und möchten die entsprechende Adresse auf Ihr Display erhalten? Senden Sie die Rufnummer an die Kurznummer 1144 und Sie erhalten in kurzer Zeit die genaue Adresse.
- Airtracker (Online-Travel-Service)
  Dieser Dienst liefert wichtige Informationen wie Gatewechsel, Flugverspätungen und An- und Abflugszeiten.
  http://www.airtracker.com
- Fahrplaninformationen (z.B SBB)
  Sie möchten die nächste Zugverbindung via SMS über Ihr Handy abfragen?
  Setzen Sie z.B. folgende gewünschte Zugverbindung ein: BERN LUZERN und senden Sie diese and die Kurznummer 222. Innert kurzer Zeit werden Ihnen die nächsten Zugverbindungen auf Ihr Display übermittelt. (Leerstellen in den Bahnhofnamen müssen mit einem Punkt dargestellt werden: z.B. Affoltern.am.Albis)
- Verkehrsinformationen
  Staunachrichten werden sofort an Natels im betroffenen Gebiet übermittelt.
  - Stauplaner Baregg
    Sie planen eine Autofahrt auf der A1 und möchten die Stauzeiten am Baregg meiden? Fragen Sie die Zeiten mit Staugefahr am Baregg ab: Schlüsselwort BAREGGZ (Richtung Zürich) oder BAREGGB (Richtung Bern) an Nummer 325 und der Stauplaner erscheint innert Sekunden auf Ihrem Handydisplay.
- Abfrage von Kontoinformationen (z.B Postphone)
  Ermöglicht es dem Kontoinhaber die letzten fünf Kontobewegungen oder das Guthaben abzurufen.
- PINFO
  Man befindet sich in Bern und sucht einen freien Parkplatz, über diesen Dienst erhält man Informationen über den Stand der verfügbaren Parkplätzen in Bern. Senden Sie das Schlüsselwort PINFO an die Kurzwahlnummer 800 und Sie erhalten die gewünschte Information.

4.4 Gateway

- Short-Message-Gateway
  Ermöglicht das Versenden von SMS in andere GSM-Netze
- Internet-Gateway
  Auf verschiedenen Internetseiten ist es möglich über Formulareingaben SMS an beliebige Personen zu versenden.
  http://www.mtn.co.za
- eMail-Gateway
  Dies ist ein für die Zukunft sehr interessanter Dienst, der es ermöglicht, sich erhaltene eMails auf sein Handy weiterzuleiten. Es besteht auch die Möglichkeit vom Handy aus Nachrichten an Emailadressen zu verschicken.
- Fax-Gateway (SMS auf Fax)
  Hier werden SMS-Nachrichten auf Fax-Geräte weitergeleitet.

4.5 Freizeit

- Sprüche (z.B Spruch des Tages)
  http://www.swisscom.ch/gd/services/mobile_com/natel/sayings-de.html
- Cocktail des Tages
  http://www.swisscom.ch/gd/services/mobile_com/natel/cocktails-de.html
- Horoskop
  http://www.swisscom.ch/gd/services/mobile_com/natel/horoscope-de.html
- Spiele
- Frage/-Antwortspiele
  http://www.swisscom.ch/gd/services/mobile_com/natel/question_answer-de.html
- Lottozahlen
  http://www.swisscom.ch/gd/services/mobile_com/natel/pilotmnc-de.html
- Veranstaltungshinweise (z.B Partys, Konzerte,...)

4.6 Swisscom Combox

4.6.1 Combox basic

Der im GSM-Netz von Swisscom Mobile integrierte Anrufbeantworter zeichnet alle eintreffenden Sprachmeldungen auf. Anrufe können auf die COMBOX basic umgeleitet werden, wenn man gerade nicht erreicht werden kann oder nicht gestört werden will. Also z.B. bei ausgeschaltetem Mobiltelefon, bei Abwesenheit, beim Aufenthalt in nicht versorgtem Gebiet oder im Besetztfall. Rund um die Uhr und weltweit. Der Eingang von neuen Meldungen wird mit einer Kurzmeldung im Gerätedisplay angezeigt. Sprachmeldungen können mit dem Handy oder jedem beliebigen Telefonapparat (Tontastenwahl) nach Eingabe des persönlichen Passwortes abgehört werden. Per einfachen Tastendruck kann man sich mit der Person, welche die Nachricht hinterlegt hat, direkt verbinden lassen.
http://www.swisscom.ch/gd/services/mobile_com/natel/combox_basic_detail-de.html

4.6.2 Combox pro

Combox pro ist ein Natel-Zusatzdienst. Er ist ein im Natel-Netz der Swisscom integrierter Swisscom integrierter intelligenter Anrufbeantworter mit vielseitigen Möglichkeiten.

Integrierte Dienste:

- Sprachspeicherung
- Faxspeicherung
- Internet-Funktionen
- Rückruffunktionen

Benachrichtigungen:

- Mittels Kurzmeldedienst (SMS)
- Mittels Pager
- Mittels E-Mail

Zugang ohne Passwort:

- Über eigenes Mobiltelefon oder 2 weitere frei definierbare Rufnummern in der Schweiz.

https://combox.swisscom.com/mms/combox_pro/combox_pro_content-de.html

4.6.2.1 Internet-Funktionen

Die Internet-Funktionalität der Combox pro bietet folgende Möglichkeiten:

- Auflistung aller Nachrichten
  - Speichern und Löschen von Nachrichten
  - Abspielen von Nachrichten
  - Faxansicht (als Grafikdatei)
  - Weiterleiten von Nachrichten als E-Mail
  - Ausdrucken von Faxen auf beliebige Faxnummern
- Veränderungen von Combox pro-Einstellungen
  - Passwort ändern
  - Sprachwahl
  - Definieren von 2 Direktzugangsnummern
  - Benachrichtigung mittels Kurzmeldedienst und/oder Paging ein- bzw. ausschalten
  - Definieren des automatischen Ausdruckens von Faxen
- Veränderung der Internet-Einstellungen
  - Ändern des Internet-Passwortes
  - Wahl des Datenformates
  - Ein- bzw. Ausschalten der Benachrichtigung mittels E-Mail

5.0 Was bringt die Zukunft...

5.1 Entwicklungen im Bereich der Satellitenkommunikation

[22]

Im Gegensatz zu den heutigen Satelliten-Kommunikationssystemen für die öffentliche Telefonie Immarsat und Intelsat, die auf geostationären Satelliten aufbauen, verwenden die neue Satelliten-Projekte den sogenannten Low-Orbit-Bereich (LEO). Geostationäre Satelliten sind in einer Höhe von rund 32'000 bis 36'000 Kilometer positioniert und man braucht eine relativ hohe Sendeleistung um sie anzusteuern, zudem sind auch die Empfangsantennen entsprechend gross. Der LEO-Bereich ist viel niedriger, er liegt bei 700 bis 1‘500 Kilometer. Hier sind die Antennen von Handy-Geräten ausreichend, um den schnellfliegenden Satelliten zu empfangen. Da sich die Satelliten aber bewegen, ist eine entsprechend hohe Zahl von diesen künstlichen Himmelskörpern notwendig, um zu garantieren, dass man an jedem Punkt der Welt, im Urwald oder in der Antarktis, stets mit Sicherheit mit wenigstens einem Satelliten Verbindung aufnehmen kann.

5.1.1 Iridum

[23]

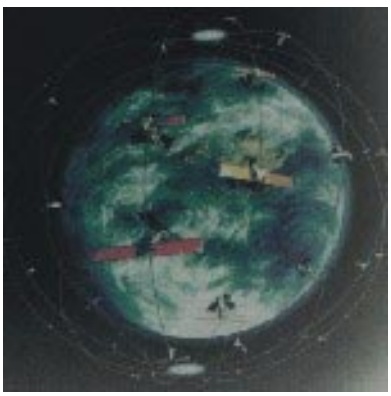


ABBILDUNG 51. Iridium Satelliten

Mit den 66 Satelliten, urspünglich waren 77 geplant, die Iridium in 6 erdnahen Umlaufbahnen in einer Höhe von 780 Kilometern positioniert und 11 Bodenstationen will das Unternehmen ein umfassendes Kommunikations-Netzwerk zur Verfügung stellen. Es soll den Kunden "jederzeit und überall, ob auf Wasser, zu Land oder in der Luft, eine(Telefon-) Verbindung in digitaler Qualität gewährleisten". Der Anwender soll mit Iridium in Regionen telefonieren oder auch Paging-Dienste nutzen können, in denen ansonsten keine Telekom-munikations-Infrastruktur vorhanden ist. Gleichzeitig wird auch Basis des GSM-Standards errichtet, also des Standards, den die grossen Netzanbieter nutzen. Iridium verbindet das Satelliten-System mit digitalen erdgebundenen Mobilfunknetzen, zum Beispiel GSM-900 und dem amerikanischen AMPS.

Die Iridium-Telefone werden von den Unternehmen Kyocera und Motorola hergestellt. Sie sollen sich im wesentlichen wie herkömmliche GSM-Handys bedienen lassen. Motorola liefert darüber hinaus einen Pager für das Satellitennetz. Als Besonderheit die Iridium-Dienste wird die Bereitstellung von nur einer einzigen Telefonnummer herausgestellt, unter der ein Teilnehmer weltweit erreichbar sein soll. Die könne seine heutige GSM-Telefonnummer sein oder eine Nummer mit dem internationalen Iridium-Zugangscode +8816. Des weiteren erhalte der Kunde nur eine Rechnung, in der sowohl die Kosten der Mobilfunk-Verbindungen als auch die Anrufe über Satellit aufgeführt sind. Nutzer sollen als Zugangsberechtigung eine GSM-Normen entsprechende SIM-Karte (Subscriber Identity Module) erhalten. Für den Einsatz in beispielsweise AMPS-Netzen ist allerdings ein

ABBILDUNG 52. Iridium Telefon

Iridium Handy notwendig. Iridium zielt mit seinem Angebot in erster Linie auf professionelle Nutzer wie vielreisende Geschäftsleute, Journalisten, Arbeiter auf Öl- oder Gasbohrinseln, Transport-Organistaionen oder Mitglieder des Katastrophenschutzes ab. Das Potential für Service gibt Iridium mit weltweit 42 Millionen Nutzern an. Die Telefondienste sollten im Herbst 1998 (23.09.1998) verfügbar sein, Fax- und Datenübertragungs-Funktionen, letztere aber nur mit einer Datenrate von 2.400 bit/s, etwa sechs Monate später. Die genannten Termine sind jedoch fraglich, da zu der hohen Ausfallsrate der Satelliten auch Probleme mit den Bodenstationen und Frequenznutzungs-Genemigungen in verschiedenen Ländern gekommen sind.

Funktionsweise des Iridium-Netzes:
Das Ka-Band dient zur Kommunikation zwischen den Satelliten (23,18 - 23,38 GHz) sowie zwischen Satelliten und Bodenstationen.

Die Übertragung zwischen Handy und Satellit finden im L-Band (1.616 - 1.626,5 MHz) statt.

http://www.iridium.com/

5.1.2 Globalstar

[22]

Globalstar ist als globales Telefonie-System vorgesehen, wobei auch hier die Dualmode-GSM-Geräte zum Einsatz kommen.

- Loral Corp./Qualcomm Inc.
- 48 LEO-Satelliten /450kg + 8 Reserven
- Höhe: 1414 km
- Start Satellitenpositionierung: 1999
- Projektkosten: 2.9 Mia$
- Zweck: Globales Telephonsystem auch mit Dualmode-Geräten (GSM)

ABBILDUNG 53. Globalstar

5.1.3 Teledesic

[22]

Teledesic ist wohl das interessanteste und ambitiöseste Zukunftsprojekt. Da hier Breitband-Kommunikation mit Datenraten von 64 Mbps im Downlink (Satellit zum Benutzer) und 2 Mbps im Uplink (Benutzer zum Satelliten) möglich sein wird. Damit dürfte Bill Gates, einer der Projektbegründer, sich seinen Traum vom ,,Information at your Fingertips" endlich weltweit erfüllen können. Mit dem Medienmogul Craig 0.McCaw hat Gates, der hier Privatvermögen, davon hat er ja wohl genügend, einsetzt, einen sehr wichtigen Partner zur Seite. Mit der Partnerschaft von Motorola, Boeing, Matra Marconi Space (Satellitenlieferant) und dem Saudi-Prinzen Alwaleed Bin Talal konnte auch die Finanzierung von 9 Mia $ gesichert werden. Anfänglich waren 840 Satelliten geplant,jetzt nur noch 288. Die Frage nach der Gewährleistung der weltweiten Abdeckung mit den entsprechenden Leistungsmerkmalen lässt sich erst nach Veröffentlichung der weiteren Detailinformationen beantworten.

- Bill Gates/ Craig O.McCaw
- Partner: Motorola, Boeing, Matra Marconi Space, Saudi Prinz Alwaleed Bin Talal
- 288 LEO-Satelliten
- Höhe: 708 km
- Start Satellitenpositionierung: 2001
- Inbetriebnahme: 2003
- Projektkosten: 9 Mia $
- Zweck: Breitbandkommunikation 64 Mbps Downlink, 2 Mbps Uplink

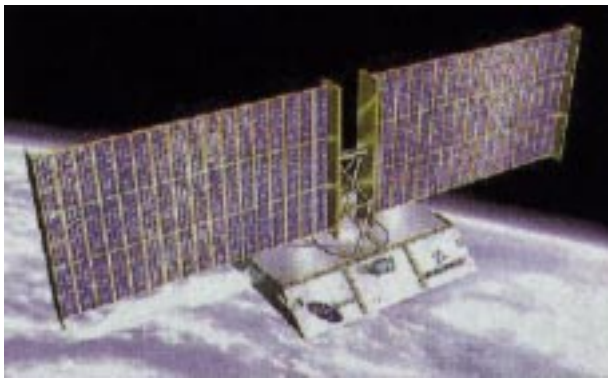


ABBILDUNG 54. Teledesic

5.2 Was werden zukünftige Mobiltelefone können ?

[31]

Heutzutage gibt es Communicatoren, die ein viel grösseres Spektrum als nur das Telefonieren abdecken. Sie haben eine eigene Tastatur und können an PCs oder Drucker angeschlossen werden. Ausserdem können sie SMS, E-Mail und Fax verschicken und empfangen. Eigentlich sind Communicatoren Palmtops mit integriertem, mobilen Digitaltelefon. Zukünftige Mobiltelefone werden immer mehr die Funktionen von Communicatoren beinhalten.
Ausserdem werden Benutzer mit MexE die Möglichkeit haben, ihre eigenen Applikationen und User Interface auf dem Mobiltelefon programmieren zu können. Schnellere Datendienste werden unsere heutigen non-voice Anwendungen wie z.B. SMS verbessern. Anstatt z.B. ab und zu per SMS Informationen abzurufen, wird es mit GPRS oder UTMS möglich sein, seine Informationen im Internet zu suchen. Heutzutage kann der Empfang eines E-Mails per SMS auf dem Mobiltelefon angezeigt werden. In Zukunft wird das ganze Mail übertragen. Internet wird das primäre Kommunikations-Interface für alle Applikationen sein. Aussendienst Mitarbeiter werden anstatt mit dem Notebook mit ihren GPRS oder UMTS Terminals im Internet elektronische Rapporte ausfüllen.

6.0 Literaturverzeichnis

[1] The GSM System for Mobile Communications, M.Mouly, M.B. Pautet, ISBN 2-9507190-0-7
[2] An Introduction to GSM, M.Redl, K.Weber, W.Oliphant, Artech House Publishers ISBN 0-89006-785-6
[3] GSM System Engineering, Asha Mehrotra, Artech House Publishers ISBN 0-89006-860-7
[4] GSM Global System for Mobile Communication, J.Eberspächer/H.-J.Vögel, B.G.Teubner Stuttgart, ISBN 3-519-06192-9
[5] Theodore S. Rappaport: Wireless Communication Principles & Practice IEEE Press, ISBN 0-7803-1167-1
[6] Technical realization of the Short Message Service (SMS), GSM 03.40, ETSI
[7] Point-to-Point SMS support on mobile radio interface, GSM 04.11, ETSI
[8] Subscriber Identity Module - Mobile Equipment (SIM-ME) interface, GSM 11.11, ETSI
[9] Specification of the SIM Application Tollkit, GSM 11.14, ETSI
[10] Security mechanisms for the SIM Application Toolkit, Stage 1, GSM 2.48, ETSI
[11] Security mechanisms for the SIM Application Toolkit, Stage 2, GSM 3.38, ETSI
[12] Funkschau 20/98 (18.September)
[13] Funkschau 21/98 (2.Oktober)
[14] Funkschau 25/98 (Dezember)
[15] Netz Nr.12, Dezember 98
[16] Netz Nr.5, Mai 98
[17] Netz Nr.2, Februar 99
[18] Telecom Report I/98
[19] Telecom Report II/98
[20] Elektronik 7/97
[21] Alcatel Telecom Rundschau (4. Quartal 1996)
[22] Orbit News 98
[23] Mobile Times Nr.7,Dez. 98
[24] AU-Systems SIMplified, September 1998
[25] AU-Systems SIMplified, Januar 1998
[26] Nokia TMA8 ppt Show
[27] Vorlesung Nachrichtenvermittlungstechnik 1, UNI Hanover, http:\\www.ant.uni-hanover.de
[28] Grundlagen der Nachrichtentechnik, Josef Schilter (HSR, 2.Studienjahr)
[29] Intoduction to G.S.M., Motorola European Cellulare Infrastructure Devision
[30] Vorlesung Computernetze, Prof. Dr. P.Heinzmann
[31] Aktuelles rund um neue Standards und Entwicklungen http://www.mobilesms.com/FutureFoneZone/
[32] Swisscom Prospekt über Natel Easy

7.0 Links

- Auf der GSM-World Seite sind die aktuellen Roaming-Abkommen mit den verschiedenen GSM Providern publiziert.
  http://www.gsmworld.com/gsminfo/gsminfo.htm

- Aktuelle Verkehrsmeldungen per SMS
  http://www.ruz.de/smis

- Diverse SMS angebote die laufend erweitet werden (von Minick)
  http://www.smsnews.ch

- Grosses Angebot an SMS-Services
  http://www.gin.nl

- Ob Fußball, Tennis, Formel 1 oder die Lottozahlen, Sie haben stets die neuesten Nachrichten. Egal ob unterwegs, zu Hause oder im Ausland, Sie erhalten alle notwendigen Informationen kostengünstig, schnell und direkt auf Ihr Handy.
  http://www.connect-online.ch/cnc/mob/sms/infos/daten.htm

8.0 Abkürzungsverzeichnis

A3,A5,A8	Schlüsselalogorithmen
AB	Access Burst
ACCH	Associated Control Channel
AGCH	Access Grant Channel
AMPS	Advanced Mobile Phone Services
AuC	Authentication Center
BCCH	Broadcast Control Channel
BFI	Bad Frame Indicator
BSC	Base Station Contoller
BSS	Base Station Subsystem
BTS	Base Transceiving Station
CAI	Charge Advice Information
CC	Country Code
CCCH	Common Control Channel
CDR	Call Data Records
CDMA	Code Division Multiple Access
CEPT	Conférance Européenne des Administrations
	des Postes et des Télécommunications
CN	Comfort Noise
CPU	Central Processing Unit
D-AMPS	Digital Advanced Mobile Phone Servieces
DB	Dummy Burst
DCCH	Dedicated Control Channel
DTX	Discontinouse Transmission
EDGE	Enhanced data-rates for GSM Evolution
EEPROM	Electronic Erasable Programable Read Only Memory
EIR	Equipment Identity Register
ETSI	European Telecommunication Standards Institute
FAC	Final Assembly Code
FACCH	Fast Associated Control Channel
FB	Frequenz Correction Burst
FCCH	Frequency Correction Channel
FDMA	Frequency Division Multiple Access
FTCH	Full Rate Traffic Channel
GMSK	Gateway MSC
GMSK	Gauss Minimum Shift Keying
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
	Groupe Spécial Mobile

HLR	Home Location Register
HSCSD	High Speed Circuit Switched Data
HTCH	Half Rate Traffic Channel
ISDN	Integrated Service Digital Networking
JDC	Japanese Digital Cellular
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
Kc	Cipher/Decipher Key
Ki	Subscriber Authentication Key
LA	Location Area
LAC	Location Area Code
LAI	Location Area ID
LEO	Low Orbit
LMSI	Local Mobile Subscriber Identity
LPC	Linear Predictive Coder
LTP	Long Term Predication
MCC	Mobile Country Code
MeXE	Mobile Station Application Execution Environment
MNC	Mobile Network Code
MoU	Memorandum of Understanding
MS	Mobile Station
MSC	Mobile Switching Center
MSIN	Mobile Subscriber Identification Number
MSISDN	Mobile Station ISDN Number
MSRN	Mobile Station Roaming Number
NB	Normal Burst
NDC	national Destination Code
NMSI	National Mobile Subscriber Identity
NSS	Network and Switching Subsystem
OMC	Operation and Maintenance Center
OMSS	Operation and Maintenance Subsystem
OSS	Operation Subsystem
PCH	Pageing Channel
PDC	Personal Digital Cellular
PIN	Personal Identity Number
PLMN	Public Land Mobile Network
PUD	Protocol Data Units
PUK	Personal Unblocking Number
RACH	Random Access Channel
RAND	Zufallszahl zur Authentisierung

RAM	Read Only Memory
ROM	Read Access Memory
RPE	Regular Pulse Excitation
SACCH	Slow Associated Control Channel
SB	Synchronization Burst
SC	Service Center
SCA	Service-Center-Adress
SCH	Synchronization Channel
SDCCH	Stand-Alone Dedicated Control Channel
SDMA	Space Division Multiple Access
SID	Silence Descriptor
SIM	Subscriber Identity Module
SM MO	Short Message Mobile Originated Point-to-Point
SM-TL	Short Message Transfer Layer
SM TP	Short Message Mobile Terminated Point-to-Point
SMS	Short Message Service
SMSCB	SMS Cell Broadcast
SMSS	Switching and Management Subsystem
SMS-TPUD	Short Message Transfer Protocol Data Units
SN	Subscriber Number
SNR	Serial Number
	Signal to Noise Ratio
SP	Spare
SRES	Session Keyzur Authentisierung
TAC	Type Approval Code
TACS	Derivate von AMPS
TCH	Traffic Channel
TDMA	Time Division Multiple Access
TRAU	Transcoder / Rate Adapter Unit
TMSI	Temporary Mobile Subscriber Identity
UMTS	Universal Mobile Telecommunication System
VAD	Voice Activity Detection
VLR	Visited Location Register
WAP	Wireless Application Protocol

9.0 Tabellenverzeichnis

10.0 Abbildungsverzeichnis