Messen der GSM-Dm-Kanäle mit SAGEM OT 460

1. Etwas Geschichte

Um 1985 war ein militärisches Walkie Talkie so groß wie ein Kommissbrot und auch so schwer. Wie aus der nachstehender Tafel 1 hervorgeht gab es aber 1985 auch Überlegungen wie ein digitales Mobilfunkgerät aussehen könnte. Noch Anfang der 90iger Jahre lief mein Nachbar mit einem C-Netz Mobilfunkgerät in Größe eines kleinen Koffers herum. Zur gleichen Zeit gingen die ersten GSM Netze in Betrieb.

1958	Das A-Netz, erstes deutsches Mobilfunknetznetz, wird eröffnet
1979	Die USA führen das erste Zellulare System **AMPS** in Chicago ein (analog)
1981	In Schweden startet das **N**ordic **M**obile **T**elephone System, (analog)
1982	Beginn der Entwicklung eines paneuropäischen Standards für digitalen zellularen Mobilfunk durch die ***Groupe Special Mobile*** *der CEPT*
1985	Das C-Netzt (analog) wird in in Deutschland eingeführt
1985	Erste Systemausschreibung für digitalen Mobilfunkstandard durch *GSM*
1987	Memorandum of Understanding (MoU) GSM zwischen 12 Ländern
1991	Die ersten GSM Netze in Betrieb (Auf Ausstellung Telecom 91...) (***GSM*** *steht jetzt für* ***Global System for Mobile Communication*** *)*
2000	Es existieren 357 GSM-Netze mit 311 Millionen Teilnehmern in 133 Ländern

Tafel 1: Entwicklung der Mobilfunktechnik

Es ist für technische Entwicklungen typisch, dass nicht allein wissenschaftliche Aspekte über eine Entwicklung bestimmen sondern zeitweilig auch Firmeninteressen und auch Ansichten leitender Beamter. So kam es auch, dass parallel zur intensiver Entwicklung am C-Netz durch die Fa. Siemens, z.B. bei SEL seit 1979 ein System mit digitaler Technik entwickelt wurde. Interessanter Weise unterstützte der damalige Bundespostminister Schwarz-Schilling die digitale Idee.
In Zusammenarbeit mit Frankreich wurde 1984 die Ausschreibung für den analogen Standard S900 von den Postverwaltungen beider Länder abgebrochen und ein Digitalstandard ausgelobt. Die darauf folgende Entwicklung bestätigt diese Entscheidung .
Deutschland gehörte in Europa zu den Vorreitern des Digitalen Mobilfunks.
Ein gutes Beispiel dafür ist die in Deutschland geborene Idee eine SIM-Karte einzuführen . Diese Karte, auf der die teilnehmerbezogenen Daten des Mobilfunkgerätes eingetragen sind, dokumentiert das Teilnehmerverhältnis im Mobilfunk.
Erst durch das *Subscriber Identity Module* (SIM) wird das *Mobile Equipment* (ME) zur *Mobilstation* (MS). Das SIM enthält die Datenbank des Mobiles und frei verfügbaren Speicher. In der Datenbank des SIM sind u.a. die in Tafel 2 eingetragenen Angaben gespeichert.

- Die *Personal Identification Number* (PIN)
- Der *Pin Unblocking Key* (PUK)
- Algorithmen zur Verschlüsselung (A3, A8)
- Der individuelle Schlüssel Ki
- Der Schlüssel Kc der aus A8, Ki und RAND berechnet wird
- Referenznummer für den Schlüssel (CKSN)
- *International Mobile Subscriber Identity* IMSI,
- Temporäre Teilnehmer Identität TMSI,
- Information zum Aufenthaltsort LAI,
- Information zur Netzidentifizierung NCC, MCC
- Rufnummer MSISDN

Tafel 2: Komponenten, die u. a. auf dem *Subscriber Identity Module* **SIM** gespeichert sind

Auf die in dieser Liste aufgeführten Begriffe wird im Verlaufe des Vortrags noch näher eingegangen. Auch werden wir den Inhalt einer SIM-Karte mit nobbis SIMSpy ansehen. Zunächst müssen wir uns mit dem Aufbau eines Mobilfunknetzes beschäftigen.

2. Struktur und Komponenten eines Mobilfunknetzes

Da man aus Südafrika genauso mit seinem Mobilfunkgerät nach Deutschland telefonieren kann wie aus Indien, oder Schweden, muss das Mobilfunknetz überall die gleiche (bzw. vergleichbare) Struktur aufweisen. Die wichtigsten Netzkomponenten Sind in Bild 1 dargestellt . Es sind hier vier wichtige Komponenten eines *Public Land Mobile Networks* PLMN, sowie die Bezeichnung einiger Schnittstellen aufgezeichnet.
1. Das *Mobile* (im Volksmund Handy genannt)
2. Das *Base Station Subsystem* oder auch die funktechnische Komponente des Mobilfunksystems, bestehend aus *Base Transceiving Station* BTS, *Base Station Controller* BSC und *Trancoder/Rate Adaptot Unit* TRAU.
3. Das *Network Switching Subsystem*, der vermittlungstechnische Teil mit den Datenbanken , bestehend aus *Mobile Switching Center* MSC und dem *Gateway-Mobile Switching Center* GMSC
4. das *stationäre Fernnetz*, welches weltweit das Rückgrad des Mobilfunknetzes darstellt, das auch mit dem ISDN und anderen nichtdigitalen Fernmeldesystem verbunden ist mit seiem *Signalisierungs System Nummer 7 (*SS#7).

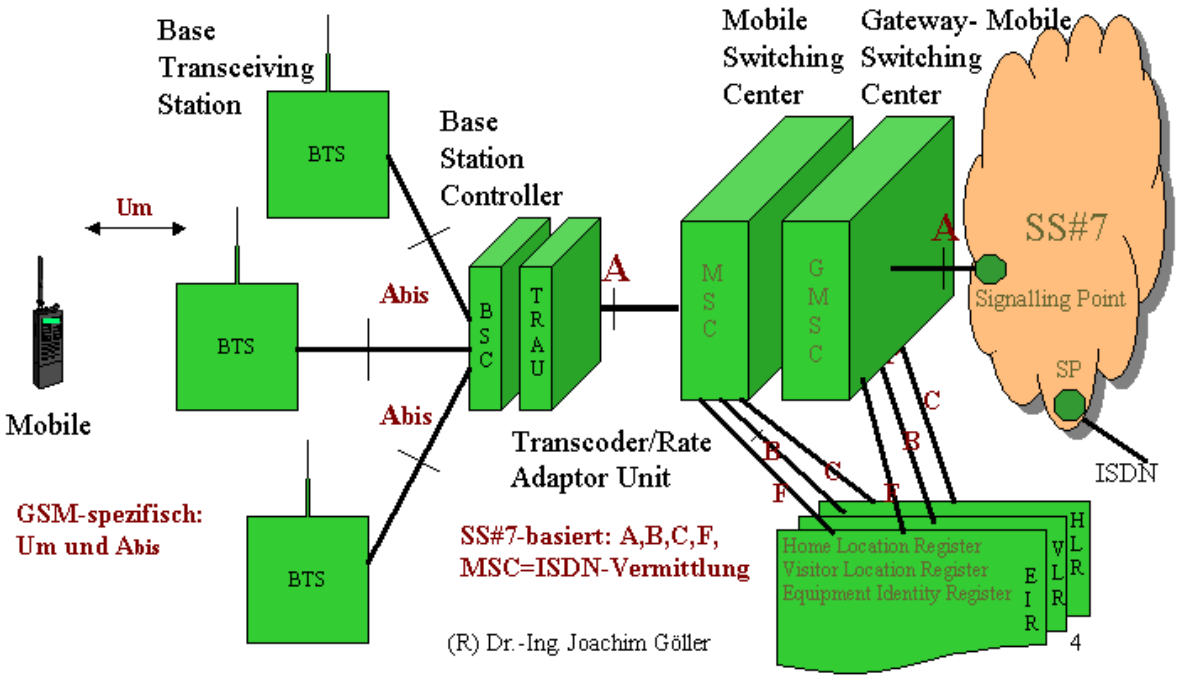


Bild1: Komponenten und Schnittstellen in einem *Public Land Mobile Network* **PLMN**

In den folgenden Ausführungen wollen wir uns mit der Signalisation auf der Luftschnittstelle „Um“ beschäftigen, der „Letzten Meile“ des Mobilfunksystems. (vergl. Der ISDN-D-Kanal, ein Lehrbrief) Das heist, wir betrachten das ganze System von der Verbraucherseite aus, weil wir im wahrsten Sinne nur die Mobilstation (MS) in der Hand haben ☺ und, weil wir das Gesagte mit Hilfe eines Trace-Mobiles auch nachprüfen können.

.

2.1 Das Mobile Equipment ME

Die MS stelltl technologisch eine Höchstleistung dar. Was die Hard- und Software des ME (mobile Equipment) betrifft, ist das auf Tafel 3 usammengefasst. Aber wie oben bereits gesagt besteht das „Handy“ ja aus ME und SIM-Karte, deren Inhalt in Tafel 2 auszugsweise, und in den Bildern 2 bis 5 etwas ausführlicher dargestellt ist.

Das Mobile ist eine, mit hochintegrierten Schaltkreisen bestückte, miniaturisierte Sende- Empfangsstation. Zu ihren Komponenten gehören:

- hochleistungsfähige Digitalfiltern, die kürzeste Umschaltzeiten zulassen,
- Schaltkreise für schnelle Signalverarbeitung und hochkonstante Oszillatoren,
- Spezialschaltkreise zur Verschlüsselung der Informationen,
- Batterien die hohe Standby Zeiten und Sende-leistungen bis 8 Watt zulassen,
- ein Display mit hoher Auflösung.

Tafel 3: Das Mobile Equipment (ME)

Das Mobile ohne Subscriber Identity Module ist somit ein Körper ohne Geist. Es ist möglich und üblich, verschiedenen Mobiles mit der gleichen SIM-Karte zu betreiben.
Von der Webseite www.nobbi.com kann man sich einen SIM-Spy herunterladen. Er gestattet einen detailierte Einblich in die Datenbank des Mobiles.

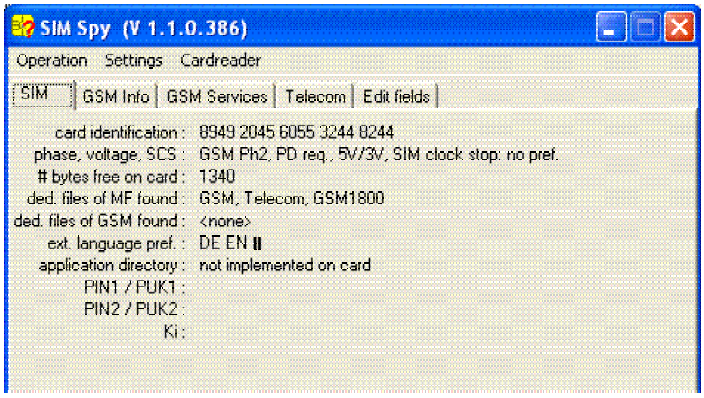


Bild 2: CALLYA-SIM-Karte, Ansicht SIM

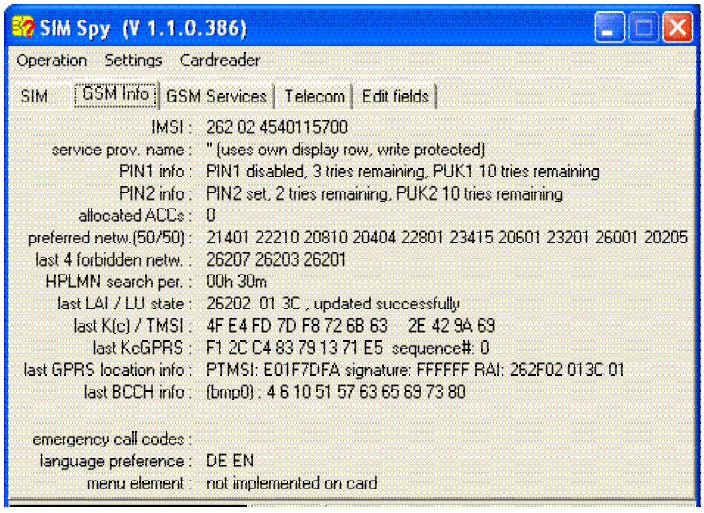


Bild 3: CALLYA-SIM-Karte, Ansicht GSM-Info

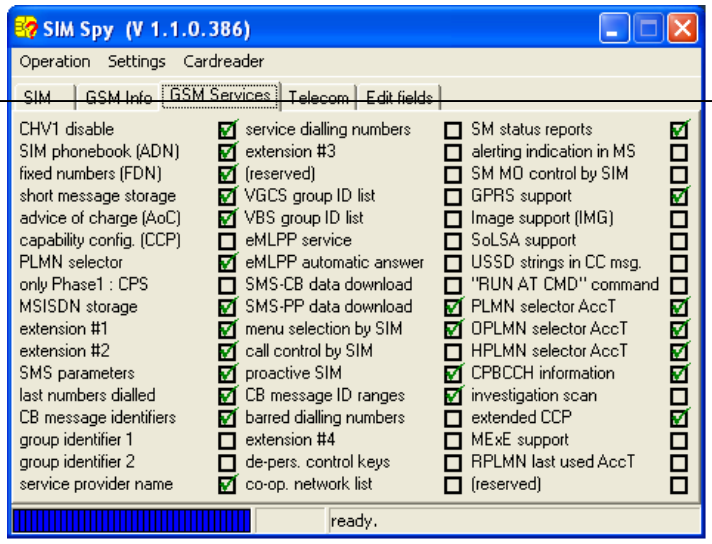


Bild 4: CALLYA-SIM-Karte, Ansicht GSM-Services

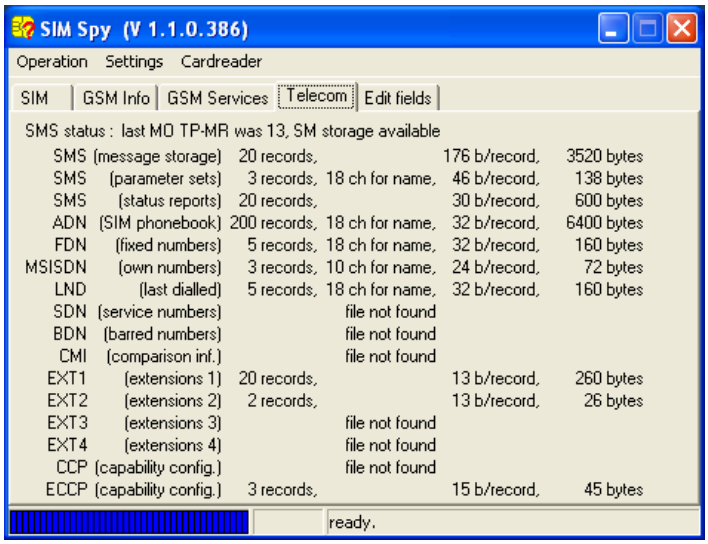


Bild 5: CALLYA-SIM-Karte, Ansicht Telecom

2.2 Die Base Transceiving Station BTS

Entsprechend Bild 1, ist die *Base Transceiving Station* der jeweilige Kommunikationspartner der MS. Das gesamte Versorgungsgebiet eines Mobilfunkbetreibers (der offiziellen Terminologie entsprechend ***Operator*** genannt) , ist in (Funk-) *Zellen* eingeteilt, von denen eine jede durch eine *Base Transceiver Station* (BTS) versorgt wird. Die *BTS* ist eine Funk-Sende-Empfangsanlage die die Luftschnittstelle (das Air-Interface) zwischen Mobile und Netz realisiert. Sie übernimmt die Fehlerschutzkodierung des Funkkanals und realisiert, analog zum ISDN, das Protokoll LAPDm auf der Schicht 2, was weiter unten genauer erläutert wird**.**

.

Die Base Station Transceiver Station (BTS)
ist eine Funk-Sende-Empfangsanlage die die Luftschnittstelle (Air-Interface) zwischen Mobile und Netz realisiert. Sie übernimmt die Fehlerschutzkodierung des Funkkanals und realisiert das Protokoll LAPDm auf der Schicht 2.
Der *Base Station Controller* (BSC)
übernimmt die Steuerung aller Geräte des BSS. In ihm ist die gesamte Intelligenz des BSS konzentriert.
Die *Transcoding Rate and Adaption Unit* (TRAU)
ist für die Komprimierung der Daten auf der Luftschnittstelle verantwortlich. Sie reduziert z.B.die Bitrate eines ISDN Kanal von 64 kbit/sec auf Bitrate der Luftschnittstelle von 16 kbit /sec beim *Full RateTransportkanal*.

Tafel 4: Bestandteile des *Base Station Subsystems* BSS

Die BTS steht nicht in jedem Falle auch geometrisch im Zentrum der Zelle. Es ist z.B. auch möglich durch drei BTS auf einem Turm, mit Hilfe von sektorisierten Antennen (Abstrahlwinkel 120^o) drei Zelle zu versorgen. Über die Organisation von *Zellen* wird noch zu sprechen sein.

2.3 Der Base Station Controller BSC

Der *Base Station Controller* (BSC) ist zentrales Element eines aus mehreren Zellen bestehenden Versorgungsbereiches. Ihm obliegt die Steuerung aller Geräte des BSS. Der BSC verwaltet die Funkkanäle seines Bereiches, informiert die MS in Form von System Informationen über alle Parameter des funktechnischen Umfeldes, analysiert die von den MS gelieferten Messwerte der Feldstärke an den verschiedenen Empfangsorten und legt danach ein erforderliches Handover fest. Eine wichtige Aufgabe besteht in der Steuerung der Anrufe an die MS (Paging).

2.4 Die Trancoder/Rate Adaptor Unit TRAU

Für die Komprimierung der aus dem ISDN mit 64 Kbit/sec kommenden Sprachdaten ist der TRAU , ***T**rancoder/**R**ate **A**dapter **U**nit* , verantwortlich. Der TRAU muss die Sprache nach einem komplizierten Algorithmus Kodieren bzw. dekodieren. Dazu sind 1.5 Millionen elementare Rechen-Operationen (Addition oder Multiplikation) pro Sekunde notwendig . Durchgeführt werden diese Operationen in Digitalen Signal Prozessoren.
Im Ergebnis der Komprimierung werden alle 20 ms Gruppen von 260 Bits übertragen, das ist eine Übertragungsrate von 13 kbit/sec.
Der TRAU ist kein Bestandteil des BSC, er ist ein selbständiges Element, das z.B. auch der BTS zugeordnet werden könnte. Es wird aber meistens, wie in Bild 1 gezeigt, zwischen BSC und MSC eingeschaltet , weil man damit zwischen BSC und BTS Übertragungskanäle einsparen kann.

2.5 Das Mobile Switching Center MSC

Das MSC ist eine ISDN-Vermittlung, wie sie im stationären Fernmeldenetz verwendet wird, die jedoch an den Einsatz im Mobilfunknetz angepasst wurde.
Das MSC übernimmt die Vermittlung der Kanäle innerhalb eines oder zwischen verschiedenen PLMN, sowie beim Handover zwischen verschiedenen MSC- Bereichen. Das MSC übernimmt auch die Protokollanpassung zwischen Call Control (ISDN-typisch) und ISUP (SS#7).
Die Modifikationen beziehen sich auf Nutzkanalzuweisungen in Zusammenarbeit mit dem BSC und auf die Funktion beim Handover zwischen verschiedenen MSC.
Während die Sprach (Datenkanäle) denen im ISDN entsprechen ist die Signalisation zwischen BSC und MSC sowie die zwischen MSC G-MSC und den Datenbanken , die im

stationären Fernnetz (SS#7) übliche, siehe Tafel 5. Wir werden uns im Zusammenhang mit den Schnittstellen zwischen den Komponenten des Netzes noch mit dem SS#7 beschäftigen .

Das *Network Switching Subsystem* (NSS) ist Zentrales Element des Mobilfunksystems an das mehrere BSS angeschlossen sind.
Seine Komponenten erledigen sämtliche Vermittlungs-, Steuerungs- und Datenbankfunktionen, die für Berechtigungsprüfung, Verbindungsaufbau, Datenverschlüsselung und Roaming notwendig sind.
Zu seine Komponenten gehören:
- Das *Mobile Services Switching Center* (MSC)
- Das *Gateway Mobile Services Switching Center* (G-MSC)
- Das *Home Location Register* (HLR)
- Das *Visitor Location Register* (VLR)
- Das *Equipment Identity Register* (EIR)

Tafel 5: Die Rolle des ***Network Switching Subsystem*** **(NSS)**

2.6 Das Gateway Mobile Switching Center G-MSC

Nur das G-MSC kann Verbindungen aus dem PLMN in andere Netzwerke herstellen. Wenn ein Anruf aus dem Festnetz einen Mobilfunkteilnehmer anruft, so initiiert das G-MSC die Teilnehmersuche über das Home Location Register und vermittelt danach an das zuständige MSC
Das *Gateway Mobile Switching Center* G-MSC stellt die Verbindung zum ISDN und anderen Stationären Netzen her. Natürlich können die Funktionen von MSC und G-MSC auch zusammengefasst sein, das hängt allein vom Betreiber des Netzes ab. Wenn z.B. ein Anruf aus dem Festnetz kommt, dann muss das G-MSC zunächst in einem *Home Location Register* HLR nachsehen, ob es einen solchen Teilnehmer überhaupt gibt, und wenn ja in welcher Zelle er sich im Moment aufhält .

2.6.1 Das Home Location Register HLR

Ein HLR kann mehrere 100.000 Teilnehmer verwalten. Ein großer Operator wie z.B. T-Mobil verfügt auch aus organisatorischen Gründen über mehrer HLR .
Die ersten beiden Ziffern der Mobile Telefonnummer stellen die Nummer des zuständigen HLR dar, in dem der Teilnehmer gespeichert ist. Im HLR sind u.a. sind folgende Teilnehmerdaten gespeichert:
- Die IMSI, vorhandene Dienstbeschränkungen, verfügbare Dienstmerkmale, die Telefon Nummer,
- Daten für den Verschlüsselungsalgorithmus und die Authentifizierung,
- Informationen für die Teilnehmersuche z.B. das aktuelles VLR usw.

2.6.2 Das Visitor Location Register VLR

Wenn ein Mobile eingeschaltet wird, meldet es sich in der Zelle an, in dem es sich gerade befindet. Bei dem nun stattfindenden *Location Update* werden die Daten des Mobiles in das „Besucherregister“ das *Visitor Location Register* VLR der zuständigen MSC eingetragen.
Natürlich erst nachdem im zuständigen HLR nachgefragt wird ob der Besitzer des Mobiles berechtigt ist am Mobilfunk teilzunehmen. Jede MSC ist mit einem VLR verbunden, jedoch können auch mehrere MSC mit dem gleichen VLR verbunden sein. Nach dieser Anfrage weiß das HLR dass sich das Mobile im Netz befindet.
Wenn der Teilnehmer nur die Zelle wechselt, aber im Zuständigkeitsbereich eines MSC d.h. VLR bleibt, dann werden nur die Teilnehmerdaten im VLR aktualisiert. Wird aber der MSC-Bereich gewechselt und damit das zuständige VLR, dann werden die Teilnehmerdaten von VLR zu VLR weitergegeben und das Home Location Register informiert.

2.6.3 Das Equipment Identity Register EIR

Genauso wie es eine eindeutige Kennung für jeden Nutzer gibt, die *International Mobile Subscriber Identity* IMSI, gibt es eine eindeutige Kennung für die Hardware d.h. das jeweilige ME, die *International Mobile Station Equipment Identity* IMEI. Mit dieser Kennung ist es möglich eine Diebstahlsicherung zu realisieren. Man sollte demnach die IMEI seines Mobiles durch Eingabe von *#06# abfragen und aufschreiben Wenn das Mobile gestohlen wird könnte man das den Netzbetreibern melden. Die IMEI des gestohlenen Gerätes kann dann in die „Schwarze Liste“ des *Equipment Identity Register* EIR eingetragen werden Es gibt dann noch eine weiße Liste, die alle zugelassenen Mobiletypen enthält und eine graue Liste erlaubt die Verfolgung dort eingetragener Mobilstationen.
Wenn nun der Dieb mit einer eigenen SIM-Karte das gestohlene Mobile betreibt (da die gestohlene SIM-Karte durch fasche Eingabe der PIN unbrauchbar geworden ist) , kann der Dieb oder der Hehler ermittelt werden.
Der Einbau eines EIR ist teuer. Da die Mobile Hardware inzwischen recht preisgünstig zu kaufen ist, verzichten inzwischen einige Netzbetreiber auf deren Installation.

3. Über Schnittstellen

3.1 Die Schnittstelle zwischen ME und BTS *Um*

Gehen wir in Bild 1 von links nach rechts. Da ist zunächst die Luftschnittstelle Um, auch Air-Interface genannt. Waren es im ISDN vor allem Meldungen und Informationselemente die den Gesprächsauf- und Abbau so wie die Zuweisung von Diensten und Dienstmerkmalen ermöglichen, so kommen an der Luftschnittstelle, neben den aus dem ISDN bekannten Call Control Messages, Meldungen zur Organisation des Management von Funkverbindungen (*Mobility Management*) und ein erhebliche Anteil von Meldungen hinzu, die es ermöglichen die Funkverbindung auf und abzubauen sowie zu halten. Diese Meldungen werden *Radio Resource Messages* genannt

Mitt Hilfe eines SAGEM Trace-Mobiles vom Typ OT 460 werden wir das Geschehen auf der Luftschnittstelle mitschneiden und somit detaillierte Einsichten über die Organisation dieses Interfaces gewinnen.

3.2 Die Schnittstelle zwischen BTS und BSC (Abis)

Auf der Schnittstelle zwischen BSC und BTS dem Abis-Interface werden PCM-Kanäle eingesetzt, wobei ein Byte nicht mehr wie im ISDN eine Amplitude des B-Kanals beinhaltet sondern 4 Amplituden des komprimierten Sprachkanals. Es existiert der ISDN-Typische D-Kanal der eine modifizierte Schicht 2 und natürlich dem Verwendungszweck angepasste Meldungen der Schicht 3 besitzt. Die L2-Adresse besteht nach wie vor aus SAPI und TEI mit den bekannte EA-Bits und im SAPI das C/R bit.
SAPI = 0 ist wieder der Übertragung von Schicht 3 Nachrichten für die Funk-Signalisation zugeordnet (Radio Signalling RSL)
SAPI = 63 ist dem TEI Management zugeordnet
SAPI = 62 kennzeichnet Meldungen die für die Systemkontrolle und Wartung (OML, *Operation &Maintenance Link*) erforderlich sind

Die Gegenstellen des BSC sind die Sender Empfänger der angeschlossenen BTS. Jede BTS besitzt daher einen eigenen Terminal Endpoint Identifier.
In SAPI und TEI existieren die aus dem ISDN bekannten Flags EA, und C/R . Die Schicht 2 wird im Abschnitt 6.1 näher betrachtet.

Im ISDN stand an der Spitze der Schicht 3 Nachrichten der Protokolldiskriminator (08 für DSS-1). Auf der Luftschnittstelle unterscheidet der Protokolldiskriminator z.B. Radio Resource (RR), Mobility Management (MM) oder Call Control (CC) Meldungen. Beim Abis –Interface steht an dieser Stelle der Message Discriminator. Damit werden die zwischen BSS und BTS zu

transportierenden Meldungstypen unterschieden. Unter anderem wird mit dem T-Bit festgelegt, ob die Meldung von der BTS zum Mobile durchgereicht , oder die Meldung in der BTS weiterverarbeitet wird. Die durchgereichten Nachrichten sind mit dem Primitiven im ISDN vergleichbar, die der Kommunikation zwischen den Schichten dienen.
In Bild 6 ist der grundsätzliche Aufbau der Schicht 3 Nachricht auf dem Abis-Interface dargestellt. Im Message Discriminator werden die 5 dargestellten Meldungstypen angezeigt. Die Meldungen bei denen T = 0 ist, werden in der BTS für den Aufbau von Meldungen auf der Luftschnittstelle verarbeitet.
Im Bild 6 sind nur drei Beispiele von 43 Meldungen dargestellt. Die Kanalnummer ist stets „1“. Es wird jeweils der zu verwendente Kanaltyp und die die Nummer des Zeitschlitzes angegeben. Alle diese hier genannten Begriffe sowie die Informationselemente werdenspäter im Text ausführlich behandelt.
Eine detaillierte Beschreibung aller Meldungen auf dem Abis Interface finden Sie in [2]. In diesem Text wollen wir nur solche Elemente des Mobilfunknetzes genauer besprechen, die wir experimentell mit unserem Trace Mobile nachprüfen können.

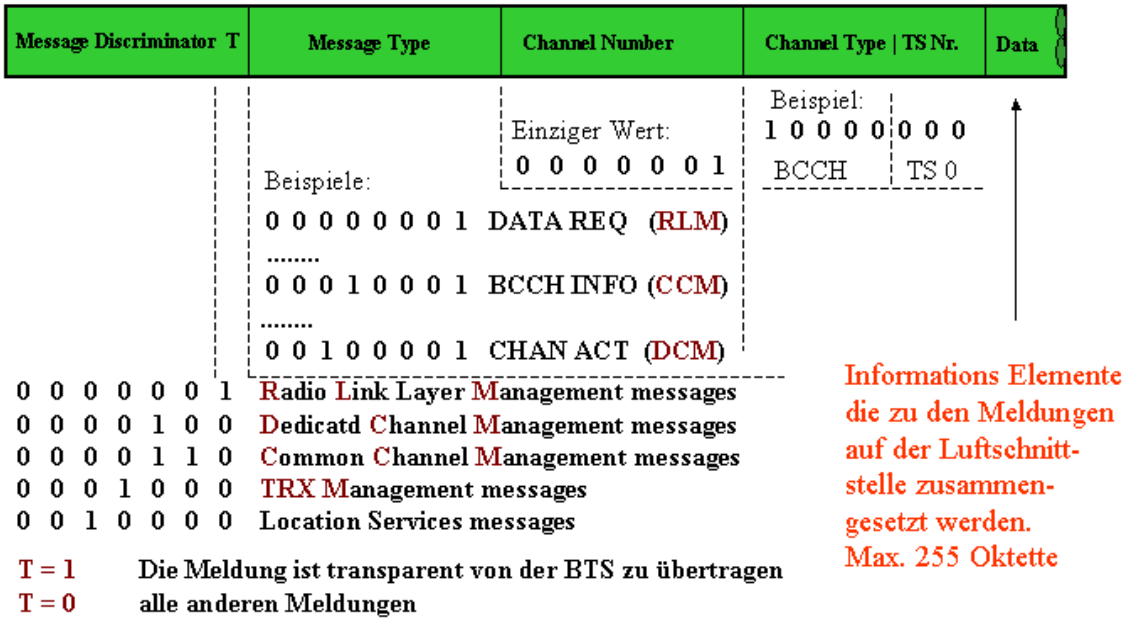


Bild 6: Protokolldiskriminatoren auf der Abis Schnittstelle

Die in Bild 1 eingezeichnete Interface A- F sind SS#7 typisch. Das ist erforderlich, damit national und international z.B. auf die Register zugegriffen werden kann. Wird z.B. das Mobile eines deutschen Reisenden, in einer Großstadt in Indien eingeschaltet, so versucht es sich im dortigen Mobilfunknetz anzumelden. Dabei wird über das Signalisationssystem des internationale Fernsprech-Fernnetzes das *HLR* des Operators in Deutschland nach den benutzerrelevanten Daten abgefragt, womit u.a. sichergestellt wird, dass das Gespräch auch bezahlt wird.
Bei Vorhandensein (innerhalb weniger Sekunden) einer befriedigenden Antwort erfolgt das *Location Update*, das Einloggen ins Netz.

4. Einige Ausführungen zum Signalisierungssystem Nr. 7

4.1 Die Trennung zwischen Signal und Zeichenkanal

Wie gesagt stellt das Fernnetz mit seiner Signalisation das Rückgrad des Mobilfunks dar. Wie bereits im Zusammenhang mit dem Abis Interface ausgeführt, sollen hier nur grundsätzliche Zusammenhänge erklärt werden. Details zum Thema Signalisation im Fernnetz sind in [2] enthalten. Es wird vorausgesetzt, dass der Leser den auf der gleichen Webseite enthaltenen Lehrbrief über den ISDN-D-Kanal gelesen hat.
Das wichtigste ist zunächst, dass im Fernnetz nicht mehr, wie im ISDN – Basisanschluss üblich, die Signalisation und die Daten gemeinsam in der Schicht 1 transportiert werden. Es ist vielmehr so, wie es sich in einer ISDN-Primärgruppe bereits abzeichnet, dass es einen getrennten Signalkanal gibt. Das ist in der ISDN-Primärgruppe von den 32 Kanälen der Kanal 16.
Im Fernnetz geht man noch einen Schritt weiter, hier liegen die Signalkanäle in gegenüber den Sprach-, bzw. Datenkanälen unterschiedlichen Trägermedien und verlaufen zum Teil auf unterschiedlichen Strecken (Bild 7). Der Zugang zu den Zeichenkanälen erfolgt über sog. Signalling Points (SP). Die Zeichenkanäle werden in Signalling Transfer Points vermittelt.
Abstrahieren wir noch weiter und betrachten wir nur noch das Signalisierungsnetz und beziehen die Netze der Mobilfunk-Operatoren mit ein.

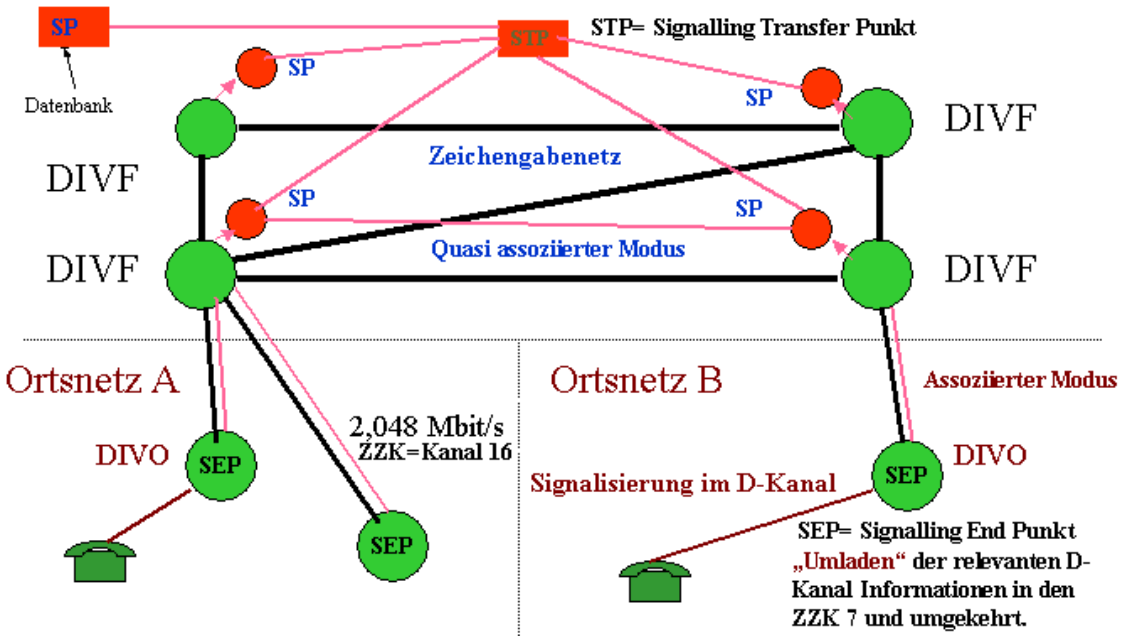


Bild 7: Das digitale Fernmeldenetz

In Bild 8 ist dargestellt wie verschiedene nationale und internationale Zeichengabenetze miteinander verknüpft werden. Im Bild 8 bedeuten SPC den *Signalling Point Code,* die Nummer die der Signalisierungspunkt im jeweiligen Nummerierungsplan besitzt. Die viereckigen Kästchen stellen Signalling Transfer Punkte dar. Als ISPC sind die Codes der Transferpunkte zum Internationalen Fernnetz bezeichnet.
Bemerkenswert ist die Lösung des Zusammenfügens nationaler Teilnetze über das „Deutsche Zeichengabe Zwischennetz".
Die in Bild 8 enthaltene Bezeichnungen NI, die von National 0 im Zwischennetz nach National 1 wechselt wird im Zusammenhang mit Bild 9 erklärt

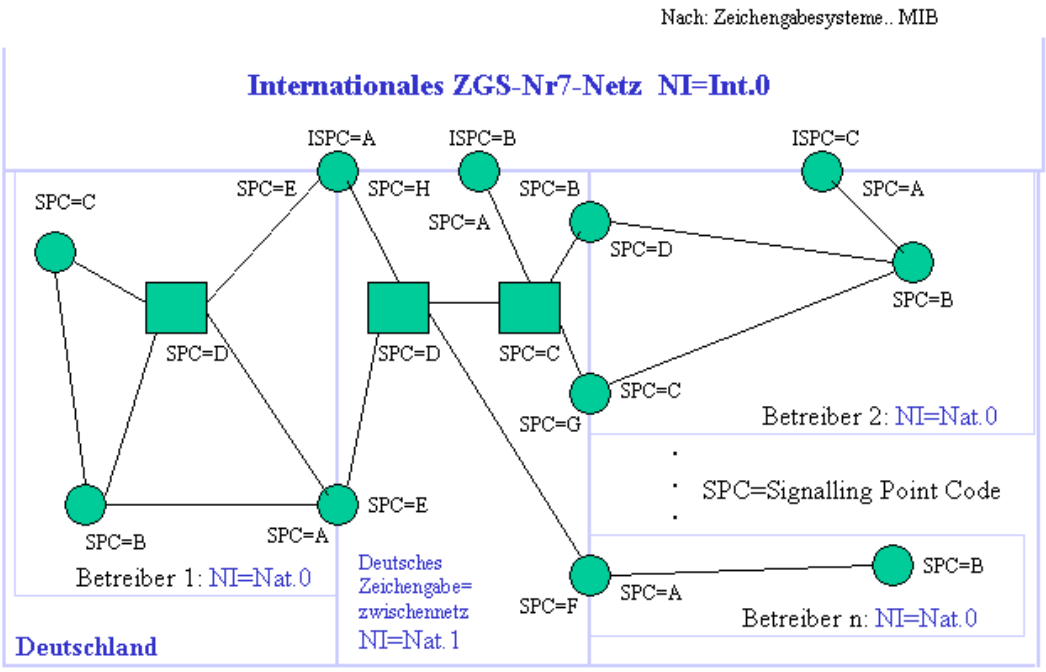


Bild 8: Internationales Zeichengabe- System- Nr.-7 Netz

4.2 Die Message Signal Unit MSU

Steuerungs-Informationen werden im SS#7 in der sog. *Message Signal Unit* MSU transportiert,

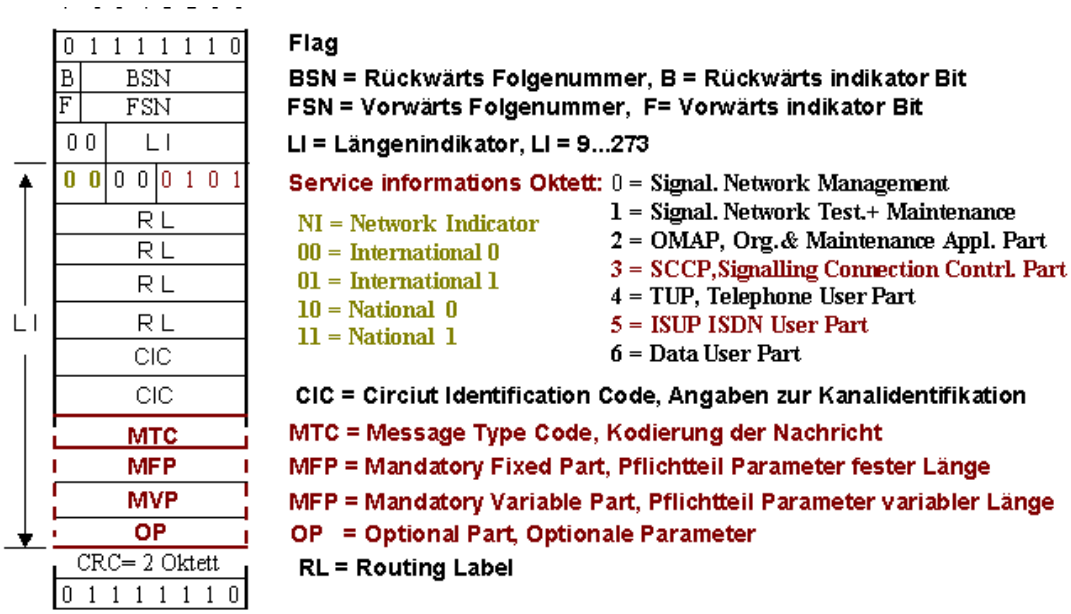


Bild 9: Die Message Signal Unit MSU

die ihrerseits Bestandteil des *Message Transfer Parts* MTP ist. Der Aufbau eines MSU Rahmens ist in

Bild 9 dargestellt
Obwohl der Aufbau des Rahmens anders ist, als der aus dem ISDN bekannte, finden wir doch, anders geordnet, die Elemente eines ISDN Rahmens wieder. Zunächst natürlich Anfangs- und Ende-Flag und das Feld für den CRC.
Die Nummerierung der gesendeten und der empfangenen Rahmen erfolgt über Rückwärts Folgenummer und Vorwärts Folgenummer. Der Längenindikator zählt aus historischen Gründen nur bis 62 und wird nicht berücksichtigt , es können bis 273 Oktett untergebracht werden.
Was in den nun folgenden Feldern transportiert wird, ist im *Service Informations- Oktett* angegeben.
Die hier dargestellte Einteilung ist auf den *ISDN User Part* ISUP zugeschnitten.
Die ersten zwei bit des *Service Informations- Oktett* stellen den *Network Indicator* NI dar.
Mit ihm ist unterscheidbar ob man sich im nationalen Netz oder im nationalen Zwischennetz oder im internationale Netz befindet.
Die *Routing Label* sind Bestandteil aller zu transportierenden Informationsarten. Sie bestehen aus der Adresse des Absender SP, dem *Origination Point Codes* OPC und der Adresse des Ziel SP, des *Destination Point Codes* DPC. Beide Codes haben eine Länge von 14 bit. Die übrigen 4 bit bilden das *Signalling Link Selection* (SLS) Feld. Es gestattet die Last gleichmäßig auf mehrere Links zwischen zwei SEP zu verteilen.
Die zwei Oktett *Circuit Identification Code* CIC geben bei Transport des ISUP in der MSU an, in welchen Kanälen die zur Signalisation gehörenden Nutzdaten transportiert werden.
Die danach rot markierten Felder beinhalten die Meldung und die Informationselemente.
Die Begriffe: Mandatory Fixed Part, Mandatory Variable Part und Optional Part. werden wir auch in den Mobilfunkmeldungen vorfinden. Es geht einfach darum Platz zu sparen. Wenn ein Informationselement unbedingt in einer Meldung enthalten sein muss, dann braucht man in der Beschreibung des Meldungsaufbaus nur noch festzulegen dass es sich um ein Pflichtelement handelt (M= Mandatory) und dazu, wenn es eine feste Länge besitzt, diese anzugeben. Alle diese Meldungen bilden hintereinander den *Mandatory Fixed Part* an Informationselementen. Man beachte, dass hier weder der Name des IE noch dessen Länge im Trace erscheint.

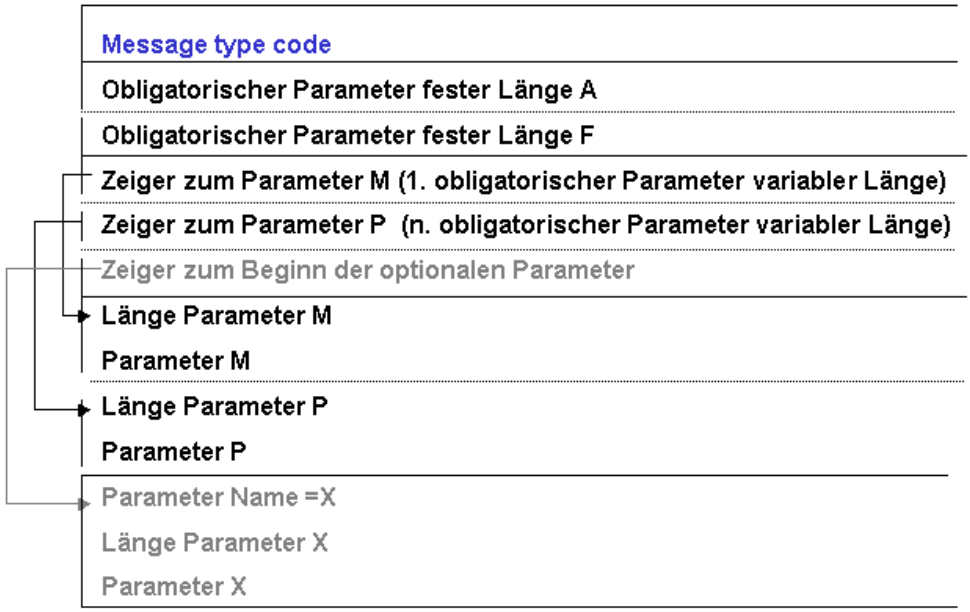


Bild 10: Mandatory Fixed Part, Mandatory Variable Part und Optional Part

Im *Mandatory Variable Part* stehen dann die Pflicht IE die, wie z.B. eine Telefonnummer, unterschiedlich lang sein können. Bei diesen IE steht kein Name aber die Länge.

Den optionalen Teil (*Optional Part*) bilden die IE die vorhanden sein können oder nicht. Diese müssen natürlich mit Name und Länge angegeben werden wie wir es aus dem ISDN gewohnt sind. Nun gibt es im SS#7 dazu noch die in Bild 10 dargestellte Erleichterung.
Nach dem Block der Pflichtparameter fester Länge stehen Zeiger die auf den Beginn eines jeden Pflichtparameters variabler Länge und auf den Beginn des Blocks der optionalen Parameter weisen.
Im Mobilfunk wird an der Einteilung in Pflicht-IE fester und variabler Länge und optionale IE festgehalten, aber ohne Zeiger zu verwenden.

Das SS#7 wurde bisher nur am Beispiel des ISUP erklärt, im nächsten Abschnitt soll daher kurz auf den Signalling Connection Control Part SCCP eingegangen werden.

4.3 Der Signalling Connection Control Part SCCP

In diesem Fall wird nicht ein ISUP transportiert (Service Informations- Oktett = 5) sondern ein Rahmen den wir Signalling Connection Control Part SCCP nennen (in Bild 9: SIO = 3). Das ist in komprimierter Form in Bild 11 dargestellt. Danach ist der SCCP Rahmen nahezu identisch mit dem Aufbau des ISUP Rahmens. Es fehlt nur die Angabe des CIC.

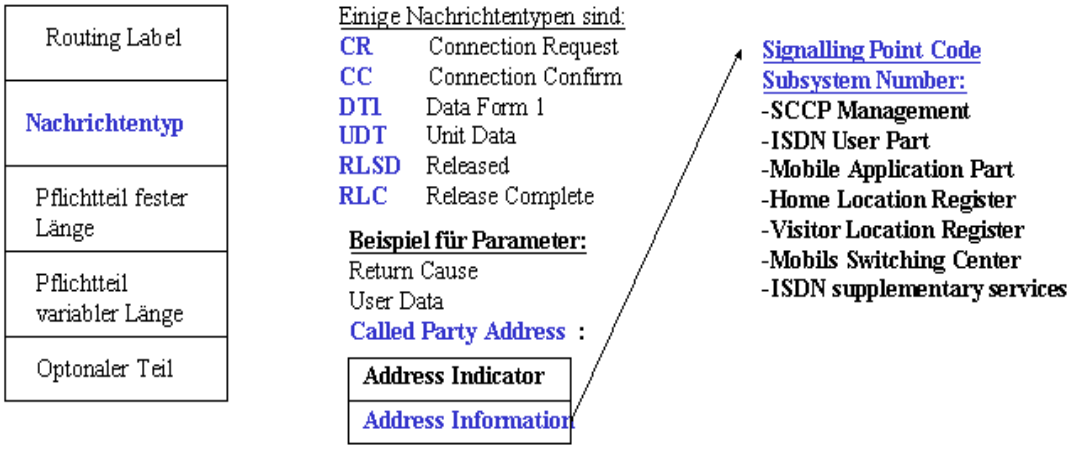


Bild 11: Signalling Connection Control Part (SCCP)

Wie man sieht, könnte als Meldung ein *Connection Request* stehen und im Address Parameter Die Adresse des gewünschten HRL.
Nach dem Verbindungsaufbau werden Daten übertragen und danach die Verbindung wieder freigegeben.
Im A-Interface wird noch weiter differenziert. Wenn Nachrichten zwischen BSC und MSC ausgetauscht werden, so wird ein *Base Station Subsystem Management Application Part* BSSMAP definiert dessen Meldungen in SCCP Rahmen transportiert werden.
Auf den Schnittstellen des NCC die nicht zur BSC gerichtet sind (vergl. Bild 1) wird ein *Transaction Capabilities Application Part* TCAP vom SCCP transportiert, der wiederum den sog. *Mobile Application Part* MAP trägt. Wie oben erwähnt ist, es mit den dem Autor zur Verfügung stehenden Mitteln, nicht möglich in die obere Netzebene hineinschauen. Deshalb soll die Beschreibung der Signalisationsmethoden in der oberen . Ein gute Beschreibung dieser Zusammenhänge finden Sie in [2].
Man sollte sich zumindest soviel merken, dass es ein weltweites Zeichengabenetz gibt, dass dort Pakete mit Steuerungsinformationen ausgetauscht werden, und dass in diese *Message Signal Units* je nach Signalisationsaufgabe weitere Pakete (SCCP, TCAP, MAP ..) eingeschachtelt sind.

5. Die Schicht 1 auf der Luftschnittstelle im GSM

5.1 Die Frequenzen im GSM 900

Ein Kanal im GSM besteht aus einer Frequenz und einem Zeitschlitz. Betrachten wir zunächst den Frequenzplan für GSM 900 auf Bild 12

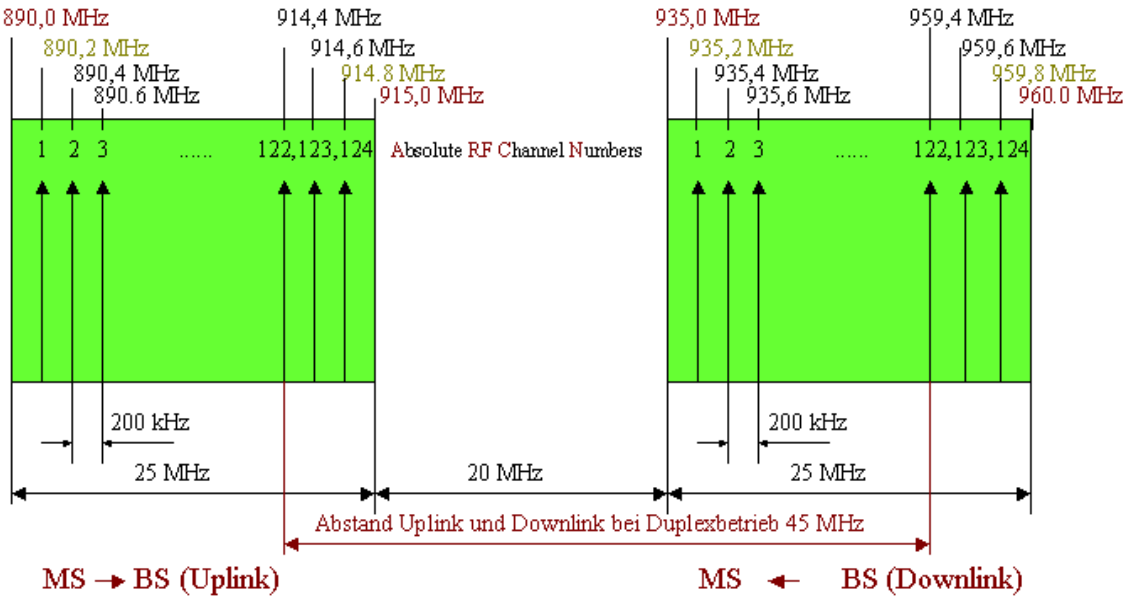


Bild 12: Frequenzplan GSM 900

Man erkennt die beiden Frequenzbänder für Uplink (890,2-915 MHz) und Downlink (935,2-960 MHz) die einen Abstand von 20 MHz voneinander besitzen.
Den Frequenzen sind Kanalnummern (sog. ARFCN = *Absolute Radio Frequency Number*) von 1 bis 124 zugeordnet, die bei der Anforderung oder in Meldungen anstelle der expliziten Frequenz verwendet werden.
Ist die ARFCN =n bekannt, so berechnet sich die absolute Frequenz

für den Downlink: F(DL) = (935,2 + 0,2*(n-1) MHz
für den Uplink: F(UL) = (890,2 + 0,2*(n-1) MHz.

Es existieren noch drei weitere Frequenzbänder. Das DCS-1800-Netz wurde 1993 durch den Operator E-Plus in Betrieb genommen. Es besitzt die Downlinkfrequenzen 1805 –1880 MHz, sowie die Uplink-Frequenzen 1710-1785 MHz. Ihm sind die 374 Kanäle von 512 bis 885 zugeordnet. Man rechnet bei bekannter Kanalnummer:

für den Downlink: F(DL) = (1805,2 + 0,2*(n-512) MHz
für den Uplink: F(UL) = (1710,2 + 0,2*(n-512) MHz.

Das dritte Band ist das PCS 1900, das z.B. in den USA verwendet wird. Es verfügt über 299 Kanäle in den Bänder Downlink 1930 – 1989,6 MHz und Uplink 1850-1909,6 MHz..

Als 4. Band muss das Extended GSM-Band erwähnt werden, dass als letztes mit den Kanälen n=975 – 1023 definiert wurde. Es gilt

für den Downlink: F(DL) = (935,2 + 0,2*(n-1024) MHz
für den Uplink: F(UL) = (890,2 + 0,2*(n-1024) MHz.

Die meisten Mobilfunkstationen arbeiten nicht im E-GSM.
Wegen der begrenzten Reichweite der Sender auf den o.g. Frequenzen können bei geographisch angemessenen Abstand der Sender, alle Frequenzen wiederverwendet werden.

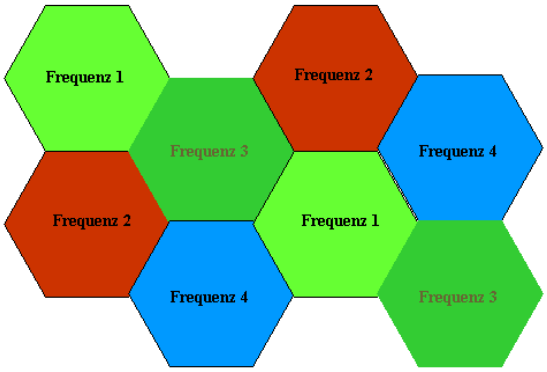


Bild 13: Das Zellularprinzip

Dazu wird das Territorium in Bereiche eingeteilt, sog. Zellen (Durchmesser 300 m bis 35 km), wobei benachbarte Zellen über von einander verschiedene Frequenzbündel verfügen. Zellen mit gleichen Frequenzen sind durch mindestens eine Zelle mit eben diesem verschiedenen Frequenzbündel. getrennt. (Bild 13).
Welche Frequenzen in einer Zelle (an einem Orte) zur Verfügung stehen, läßt sich z.B. mit einem SAGEM Trace-Mobile (z.B. vom Typ OT 460) feststellen. Wird das Mobile an einen PC angeschlossen auf dem das Programm OT Drive 4 implementiert ist, und der Betriebsmode Scanning eingeschaltet, so kann man ansehen, welche Sender mit welcher Feldstärke am Ort zur Verfügung stehen.
Betrachten Sie dazu eine Aufzeichnung die der Autor im Neubaugebiet in Königs Wusterhausen gemacht habe.

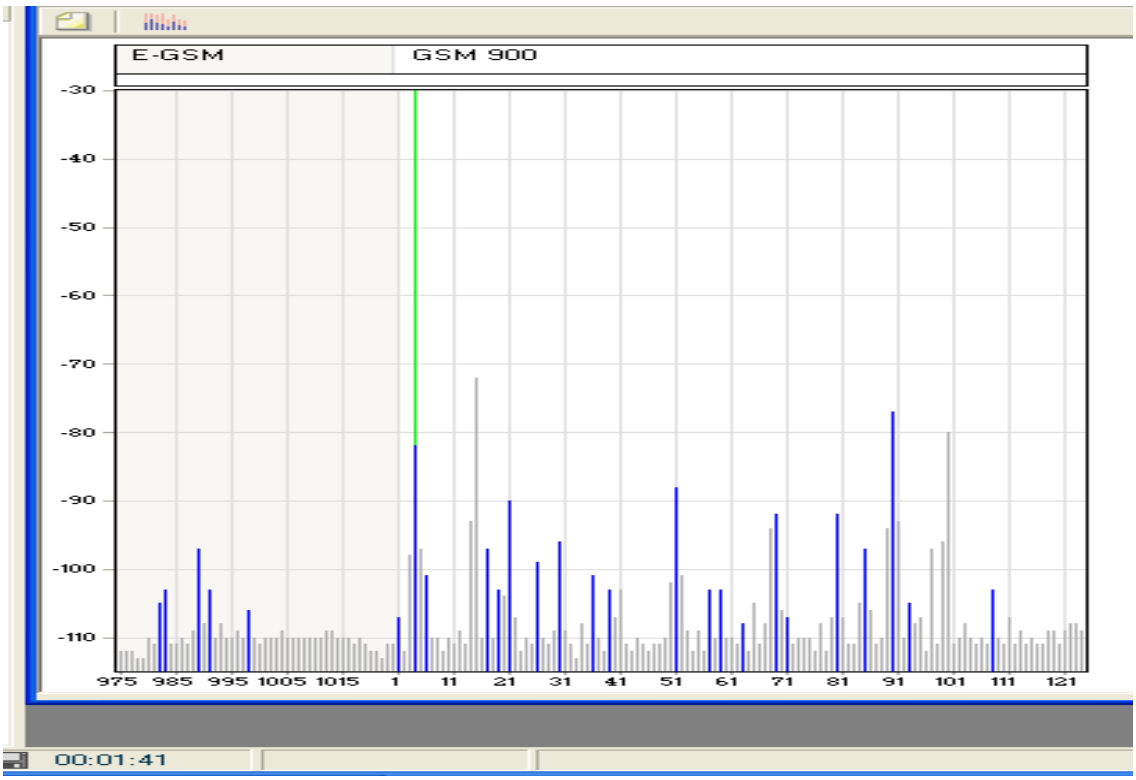


Bild 14: Feldstärken auf E-GSM und GSM-Kanälen im Neubaugebiet Königs Wusterhausen

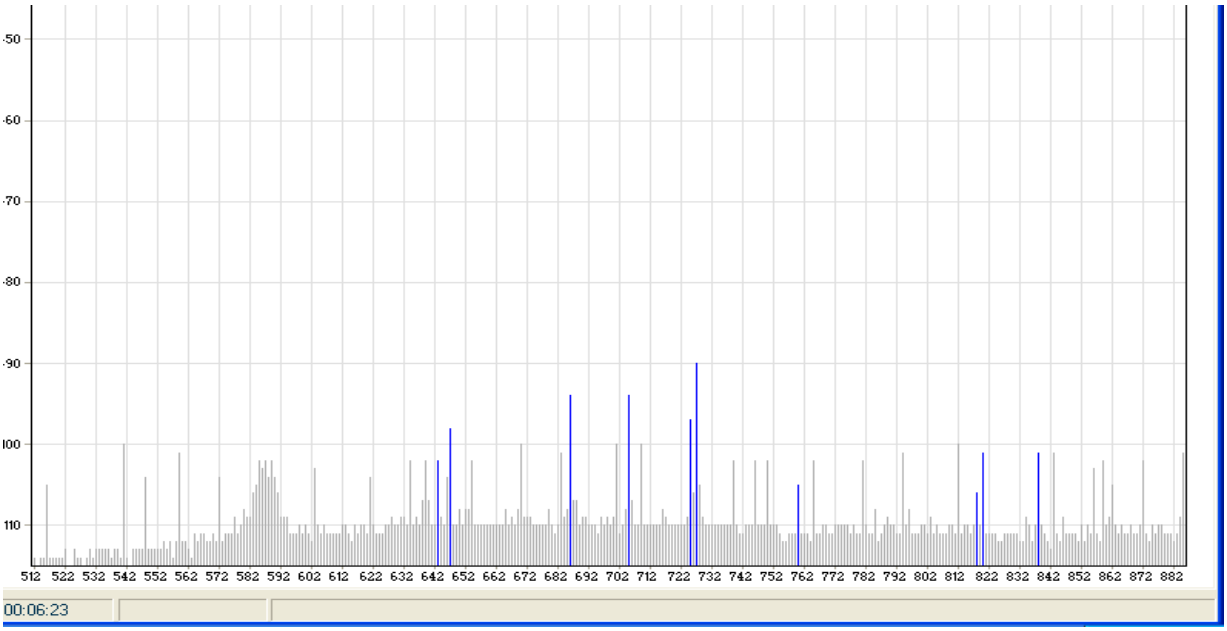


Bild 15: Feldstärken auf DCS-Kanälen im Neubaugebiet Königs Wusterhausen

Die in den Bildern 14 und 15 dargestellten (gemessenen) Feldstärken sind eine Momentaufnahme, In Wirklichkeit atmet die Bilder aufgrund der schwankenden Ausbreitungsbedingungen, d.h. die Striche ändern Ihre Länge.
Damit Sie eine Vorstellung davon besitzen, wie groß die Feldstärke sein muss, damit sie für eine Mobilfunkverbindung nutzbar ist, sei im Vorgriff gesagt, dass die Mobilfumkanbieter einen Mindestempfangspegel von –106 dBm verlangen.
Wie aus den Bildern 14 und 15 zu erkennen ist, sind es nur wenige Frequenzen, die die –100 db Marke überschreiten.
Die Blau eingezeichneten Spektrallinien stellen sog. Bakenfrequenzen, das *Funkfeuer* der BTS, dar (Abschitt 5.5). Eine jede BTS besitzt solch eine Bakenfrequenz, auf die sich ein Mobile, nach dem Einschalten, bei der Suche nach einer Gegenstelle einstellt um von dort alle wichten Informationen (System Informationen) seines elektronischen Umfeldes zu empfangen.
Die grüne Linie im Bild 14 ist ein Zeiger mittels dessen eine Spektrallinie abgedeckt werden kann, worauf (im Fenster Bild 14 abgeschnitten) Kanal und Feldstärke explicit angezeigt werden.

Berücksichtigt man, dass das GSM 900 Frequenzband mit seinen 124 Kanälen noch unter den verschiedenen Operatoren aufgeteilt wird, so muss folglich eine Methode gefunden werden die relativ wenigen Frequenzen effektiver zu nutzen.
Das geschieht, wie oben bereits erwähnt, durch Zeitteilung oder TDMA (Time Division Multiplex Access) . Betrachten Sie dazu Bild 16.

5.2 Die Zeitteilung auf den Frequenzen des Mobilfunknetzes

Die Übertragung auf dem Funkkanal erfolgt über die Aneinanderreihung von Impulsbündeln die Bursts genannt werden. Die Burstlänge von 15/26 ms wird später erklärt. Das Extrahieren von Impulsen aus einem Datenstrom und Bildung eines neuen Kanals dürfte aus dem ISDN bekannt sein, wo aus den jeweils 4 D-Bits aus einem Impulsrahmen der D-Kanal gebildet wird.

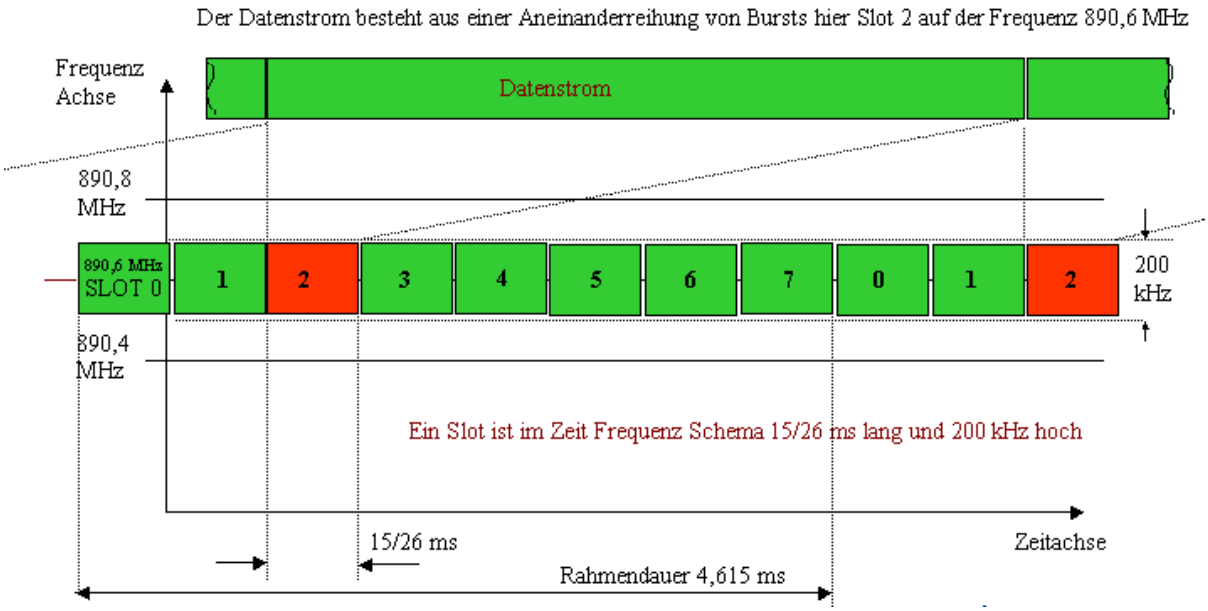


Bild 16: Zeitteilung der zur Verfügung stehenden Frequenzen

Der so entstehende physikalische Kanal muss nun für die unterschiedlichen logischn Kanäle, deren Notwendigkeit weiter unten erklärt wird, zur Verfügung stehen. Dazu wurde ein raffiniertes Zeitschema entworfen (Bild 17)

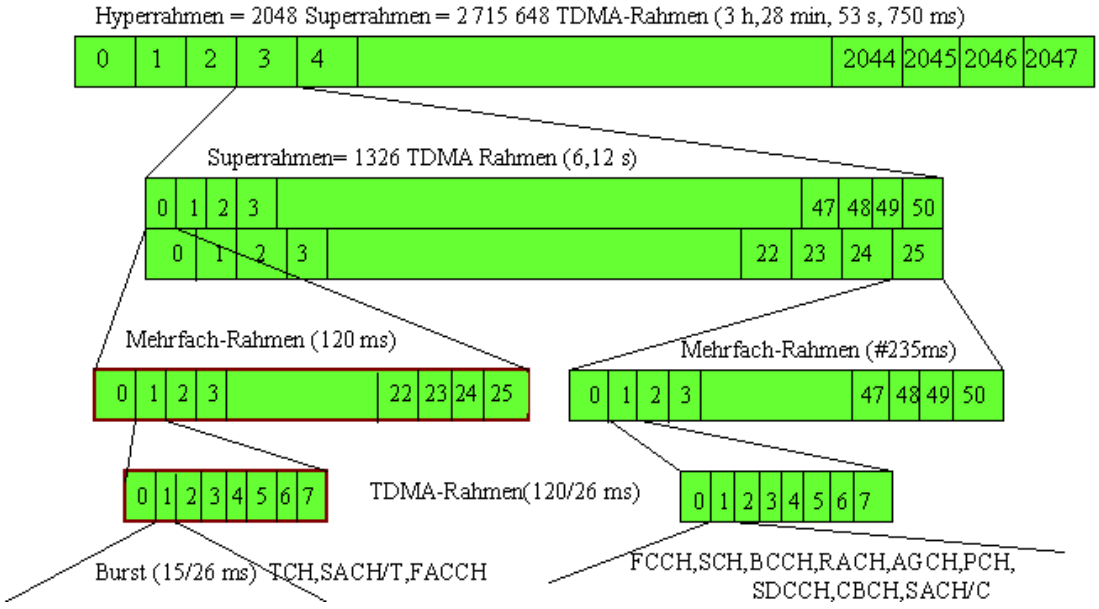


Bild 17: Rahmen Hierarchie (nach Mouly Pautet [1])

Zunächst muss von einer physikalischen Gegebenheit ausgegangen werden. Diese besteht darin, dass von der TRAU (aufgrund der Synchronisierung mit dem ISDN-Kanal) alle 120 ms ein Rahmen übertragen wird, der 26 TDMA Rahmen enthält. Somit besitzt ein TDMA-Rahmen eine Dauer von 4,615 ms und ein Burst eine Dauer von (120/26)/8 = 15/26 = 0,577 ms.
Es wäre naheliegend dieses Zeitschema einfach zu wiederholen. Die Entwickler des GSM-Systems haben sich aber das in Bild 17 dargestellte System ausgedacht. Danach werden zunächst 51 Mehrfachrahmen zu einem Superrahmen zusammengefasst und 2048 derselben zu einem Hyperrahmen. Die TDMA-Rahmen Nummer wiederhold sich also alle 3 Stunden , 28 Minuten, 53 sec

und 750 ms. Diese Hirarchie wurde gewählt, weil die Rahmennummer für die Verschlüsselung (die später zu besprechen ist) verwendet wird.
Als Konsequenz muss dem Mobile , wenn es sich am Netz anmelden will, mitgeteilt werden, welchen Kanal und welche Zeitschlitz es zugeteilt bekommt und welcher Rahmen, der 26 x 5 1x 2048 möglichen, der Aktuelle ist.

5.3 Der 26iger Mehrfachrahmen

Ähnlich wie beim ISDN-Kanal das D-Bit im Rahmen der Länge 48, wird von den 26 Bursts im Mehrfachrahmen einer der Bursts dem langsamen Signalkanal zugeordnet. In Abschnitt 5.8 wird nachgewiesen, dass 4 Burst erforderlich sind um eine Meldung zu übertragen. Meldungen auf dem Slow Associated Control Channel werden somit aller 480 Millisekunden übertragen. Eine weitere Feinheit ist aus Bild 18 zu entnehmen. In der oberen Hälfte des Bildes ist von links nach rechts die Zeitachse des 26iger Multiframe dargestellt.
Zeilenweise angeordnet, die Organisation der Bursts in den einzelnen Slots. Es wird als Beispiel angenommen dass der Slot 3 einer bestimmten Frequenz einem TCH zugeordnet sind. Es soll gezeigt werden, dass der A-Burst und der ausgelassene Burst in benachbarten Slots verschiedene Positionen einnehmen
In der unteren Hälfte des Bildes ist die Burstfolge auf dem Empfangs- und dem Sendekanal aufgeführt. Es wird nur Slot 3 betrachtet. Man erkennt zunächst, dass Empfangs- und Sendefolge um drei Bursts gegeneinander verschoben sind. Das ist notwendig damit das Mobile Zeit hat, zwischen Empfang und Senden umzuschalten.
Nun muss das Mobile während der Informationsübertragung auch noch Messungen auf den Kanälen der Nachbarzellen durchführen, um in der Bewegung feststellen zu können auf welche Frequenz gewechselt werden muss , wenn das Gerät an die Grenzen des Versorgungsbereichs der Zelle transportiert wird. Dazu stehen zwei Zeitabschnitte zur Verfügung. Ein kurzer von 4x15/26 ms (beim Umschalten von Senden auf Empfang) und ein langer, von 12x15/26 ms, der aufgrund der Lücke im 26iger Multiframe entsteht.

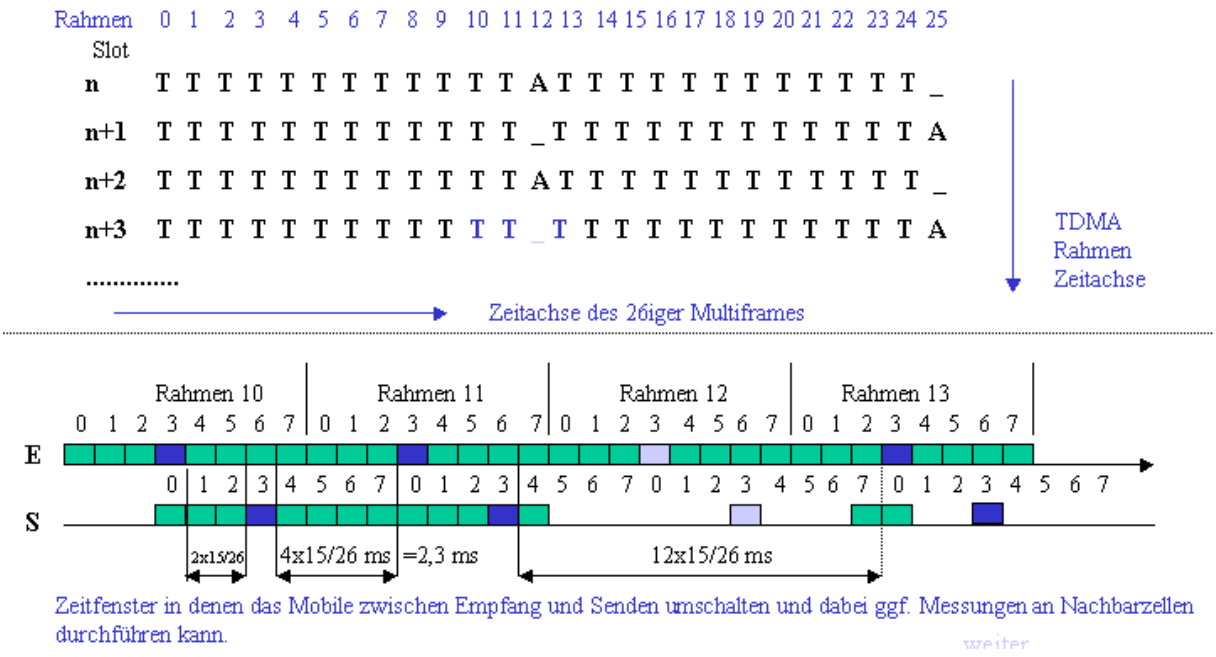


Bild 18 : Organisation des TCH/F+ SACH

Die gewonnenen Messergebnisse werden in der Meldung namens MEASUREMENT REPORT im Abstand von etwa einer Sekunde auf dem SACCH an die BTS gesendet. Wir werden uns noch ausführlich mit dieser und den anderen Meldungen im Rahmen des Verbindungsaufbaus beschäftigen.

5.3.1 Über Bursts

Man unterscheidet im GSM fünf verschiedene Arten von Bursts. Betrachten wir dazu Bild 19.

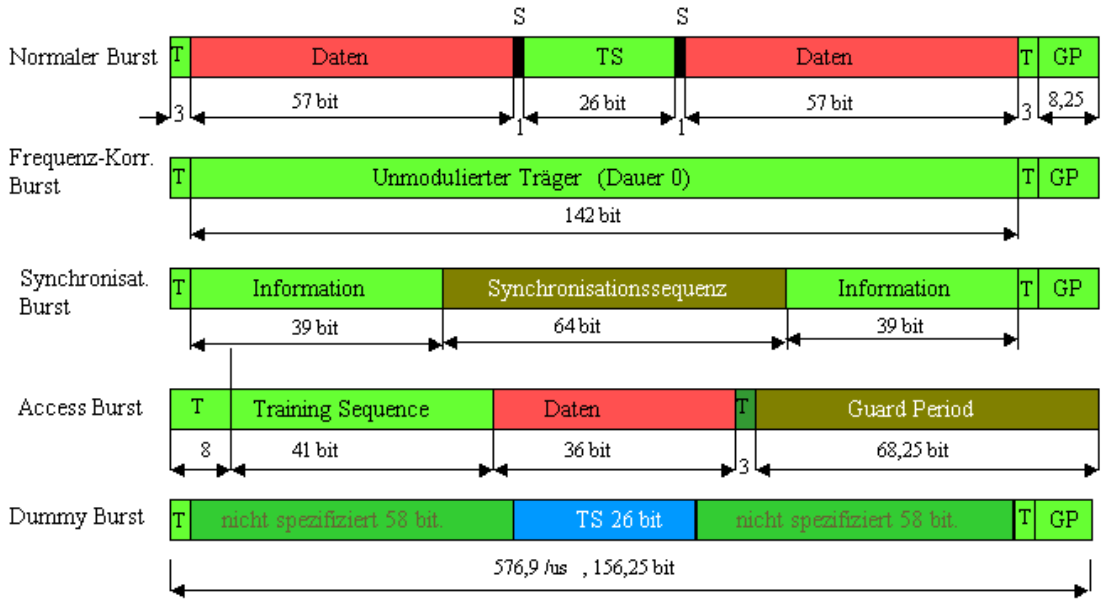


Bild 19: Bursts im GSM, S = Steeling Flag, GP = Guard Period, T = Tail Bit, TS = Trainings Sequence

Der Burst mit dem wir es bis jetzt zu tun hatten ist der *Normale Burst.* Er enthält zwei Pakete von je 58 bit, die um die sog. Trainingssequenz gruppiert sind.
In den 58 bit-Paketen enthalten je 57 bit die fehlergesicherten Nutzdaten. Ein Bit auf jeder Seite der Trainingssequenz heißt S-Flag (Stealing-Flag). Wenn in einigen Bursts des TCH das S-Flag gesetzt ist heißt das, dass dieser Burst keine Anwenderdaten transportiert sondern Steuerinformationen. Es entsteht kurzzeitig ein schneller gewidmeter Steuerkanal FACCH (*Fast Associated Control Channel*). Die Informationen die über den FACCH übertragen werden, werden weiter unten im Text ausführlich besprochen.
Die *Trainings Sequenz* ist eine Bitfolge deren Muster bei Sender und Empfänger bekannt ist. Sie wird benutzt die Parameter des Entzerrers einzustellen und auch um die Bitfehlerrate abzuschätzen. Es gibt 8 verschieden Trainings Sequenzen, die so gewählt wurden, dass ihre Bitmuster möglichst wenig übereinstimmen
Es wären noch die 3 Tail-Bits (Nullen) am Anfang und Ende des Bursts zu erwähnen. Ihre Rolle sowie die des 8,25 bit langen Schutzperiode (Guard Period) hängt mit der Physik des Bursts zusammen, der ja eine ansteigende und eine absteigende Flanke besitzt, und in dessen Bereich konstanter Leistung in der Mitte die 142 Bit Nutzinformation ausgestrahlt werden.

Der Frequency Correction Burst und der Synchronisation Burst werden beim Einschalten des Mobiles und Suchen der zuständigen BTS eingesetzt.

Der Access Burst findet bei der Kanalanforderung Verwendung und der Dummy Burst wird eingesetzt, wenn zugeordnete Zeitschlitze nicht anders belegt werden können.

.

5.3.2 Der dedicated mode

Wenn ein aktiver Kanal zwischen Mobile (MS) und Basisstation (BS) besteht, so sagt man das Mobile befindet sich im ***dedicated mode***.
Wie beschrieben wird im ***dedicated mode*** der Normalburst zum Transport von Nachrichten und Steuerinformationen benutzt.
Damit ist klar, wie der physikalische Kanal in der Phase des Gesprächs zwischen Mobile und BTS belegt wird. Dem Mobile wird eine Frequenz und ein Zeitschlitz zugewiesen auf dem dann die Bursts des TCH und des SACCH übertragen werden.

5.3.3 Der idle mode

Ist die MS eingeschaltet und verfolgt passiv das „Geschehen im Netz“ so spricht man vom ***idle mode.*** Die MS ist in Wirklichkeit in diesem Mode alles andere als müßig (idle). Sie muss: laufend mit der Basis Station in Kontakt bleiben, den sog. *Paging Kanal* abhören um zu erfahren wann an ihre Adresse ein Ruf erfolgt, sowie die funktechnische Umgebung bewerten. Letzteres erfolgt durch Lesen der Systeminformationen aus denen die aktuelle Zelle der aktuelle BCCH und die Nachbarfrequenzen hervorvergehen.

Richtung	Kanal	Bezeichnung
MS ←BS	FCCH	Frequency Correction Channel
MS ← BS	SCH	Synchronisation Channel
MS ← BS	BCCH	Broadcast Control Channel
MS ← BS	PAGCH	Paging und Access Grant Channel
MS → BS	RACH	Random Access Channel
MS ↔ BS	SDCCH	Stand-Allone Dedicated Control Channel
MS ↔ BS	SACCH	Slow Associated Control Channel
MS ↔ BS	FACCH	Fast Associated Control Channel

Bild 20: Die Steuerkanäle im GSM

Wie später erklärt wird sind beim Einschaltvorgang des Mobiles die ersten 6 Kanaltypen beteiligt.
Befindet sich das Mobile im Idle Mode sind es vorallem der Broadkast und die Paging Kanäle die abgehört werden.
Die letzten beiden Kanäle im Bild 20 werden nur im dedicated mode eingesetzt.

5.4 Der 51iger Mehrfachrahmen mit *Common Control Channel* CCCH

Bei der Besprechung des TCH hatten wir einen Mehrfachrahmen in dem pro Zeitschlitz successive 26 Normalbursts auftraten. Der Mehrfachrahmen für die Steuerkanäle nimmt 51 TDMA-Rahmen auf. Der Umstand, dass die Anzahl der TDMA Rahmen der beiden Mehrfachrahmen Teilerfremd sind, führt dazu, dass beim Messen der Nachbar Kanälen (siehe Bild18), wie erwünscht, nicht immer der gleiche Kanal getroffen wird.

Betrachten wir dazu die Burstfolge auf dem *Common Control Channel* CCCH auf Bild 17 . Man liest ab, dass die in dem 51iger Rahmen vorkommenden Bursts den *Frequency Correction Channel* , oder den *Synchronisation Channel,* oder den *Broadcast Control Channel,* oder den *PACCH* bilden. Alle diese Kanäle belegen den Zeitschlitz 0 der Frequenz des BCCH .

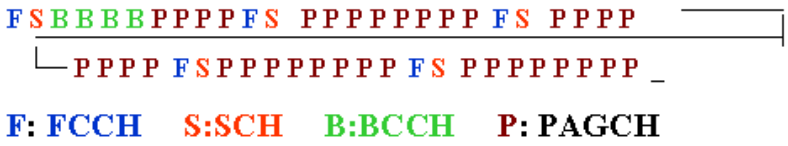


Bild 21: Burstfolge auf dem Slot 0 der *beacon frequency*

5.5 Messung und Eigenschaften des *Broadcast Common Control Chanel* BCCH

Es gibt eine *beacon frequency* (den BCCH), eine ausgezeichnete Frequenz in der Funkzelle, auf deren Zeitschlitz 0 im Downlink die Kanäle aufmoduliert sind die in Bild 17 zu sehen sind. Danach wird als erstes ein Frequency Correction Burst ausgesendet. Nach 8 Burstperioden folgt ein Synchronisations Burst. Danach folgen 4 mal Bursts die Informationen des Broadcast Control Channels tragen, danach Bursts des Paging Channels, usw.

5.5.1 Was geschieht nach dem Einschalten des Mobiles?

Das Mobile sucht nach dem Einschalten zunächst nach dem stärksten Sender, das ist meist ein BCCH. Im Zeitschlitz Null eines BCCH wird ein *Frequenzkorrektur Burst* und danach, acht Burstperioden später, ein *Synchronisations-Burst* ausgestrahlt.
Die MS wird also zunächst beim einem stärksten Sender nach dem Frequenzkorrektur-Kanal suchen und sich damit auf diesen Sender einjustieren. Da der Synchronisations-Burst 8 Burstperioden nach dem Frequenzkorrektur-Burst folgt, kann sich die MS danach auf den Synchronisationskanal einstellen
Nach Demodulation des SCH erfährt die MS die genaue Nummer des Zeitschlitzes im Zyklus der 8x26x51x2048 Burstperioden und erfährt u.a. auch den *Base Station Identity Code*s (BSIC). Der BSIC (bestehende aus 6 bit) der sich aus Network Color Code NCC und den *Base Station Color Code*s BCC zusammensetzt (je drei bit Länge)

Eine Bemerkung zum Begriff Farbcode. Er ist aus der Geographie bekannt, wo auf Landkarten politisch zusammenhängende Gebiete mit der gleichen Farbe gekennzeichnet sind.
Im GSM besteht auch eine Europakarte in unterschiedlichen Farben zur Abgrenzung der Länder. Die Farben sind hier durch Ziffern repräsentiert, den NCC. Für Deutschland ist der *Network Color Code* (NCC) 3 oder/und 7 vorgesehen.
Das ist aber nicht die einzige Klassifizierung von Ländern und Operatoren. So ist ein dreistelliger *Mobile Country Code* MCC festgelegt, der für Deutschland 262 beträgt.
Ergänzt wird dieser MCC durch den *Mobile Network Code* MNC. Dieser ist für den Operator D1 gleich „01“, für den Operator D2 gleich „02“ und für den Operator E-Plus gleich „03“

Nun zurück zum Begriff NCC. Der NCC von T-Mobile (D1) ist grundsätzlich „3“. Aber auch der NCC von E-plus ist „3“ Auseinandergehalten werden die beiden durch den Mobile Network Code MNC, der für D1 gleich „1“ und für E-Plus gleich „3“ ist.
Deutschland besitzt nun noch den NCC = 7 , der von Vodafone verwendet wird.
In der auf dem BCCH periodisch ausgestrahlten *System Information Type 2* wird dem Mobile mitgeteilt, welche BCCH Träger mit welchem NCC’s es abhören darf.

Im Trace eines Mobiles mit D1-SIM-Karte finden wir dort konsequenterweise den Eintrag (Vergl Tafel 12):

```
08  ----1---  BCCH carrier with NCC = 3 is permitted for monitoring;
```

Da Vodafon (D2) international agiert benutzt der Operator D2 auch noch die NCC's 4, 5 und 6, was man aus nachstehendem Traceauszug einer Vodafone-Verbindung ablesen kann:

```
f8  1-------  BCCH carrier with NCC = 7 is permitted for monitoring;
    -1------  BCCH carrier with NCC = 6 is permitted for monitoring;
    --1-----  BCCH carrier with NCC = 5 is permitted for monitoring;
    ---1----  BCCH carrier with NCC = 4 is permitted for monitoring;
    ----1---  BCCH carrier with NCC = 3 is permitted for monitoring
```

„NCC = 3 is permitted" bedeuted natürlich nicht, dass man mit einer SIM-Karte von Vodafone Zugang zu D1 hat.
Betrachten Sie dazu auf Bild 3 die Ansicht GSM-Info auf einer CALLYA-SIM-Karte,. Hier finden Sie dass es „forbidden" ist Verbindung mit dem PLMN 26201 (D1) aufzunehmen. Offenbar ist NCC = 3 mit einem anderen MCC erlaubt.

Wie wir erfahren haben , sind auf der SIM-Karte sind sowohl erlaubte als auch unerlaubte NCC's eingetragen. Damit wird sich das Mobile mit einer SIM-Karte von D1 z.B. nicht bei der BTS von D2 anmelden obwohl diese den stärksten Träger liefert, sondern bei der BTS von D1, die ebenfalls empfangen wurde.

5.5.2 Die Rolle des Base Station Color Code

Da es vorkommen kann, dass Sender die die gleiche BCCH Frequenz ausstrahlen, räumlich nicht so weit auseinanderliegen, dass sie von einem Mobile nicht beide gleichzeitig empfangen werden, muss es möglich sein diese Träger zu unterscheiden. Bei der Einrichtung des Netzes wird daher benachbarten BCCH mit der gleichen Frequenz eine verschiedene „Farbe" zugeordnet. Die Farbe wird durch den *Base Station Color Code* (BCC) repräsentiert.

5.6 Der 51iger Mehrfachrahmen mit *Slow Dedicated Control Channel* SDCCH

Nachdem erklärt wurde, wie das Mobile den zu seinem Aufenthaltsort gehörenden BCCH findet, wäre es folgerichtig die Anmeldung des Mobiles beim Netz, das sog. LOCATION UPDATE zu erklären. Die genaue Beschreibung diese Vorgangs soll jedoch im Abschnitt 8 im Zusammenhang mit den Meldungen des Mobility Management erfolgen. Im Moment soll nur so viel gesagt werden, dass das Mobile als erstes einen Kanal anfordert, diesen Kanal zugewiesen bekommt und auf diesem den LOCATION UPDATE REQUEST abschickt. Ehe der Request bestätigt wird, muss sich das Moblie Authentifizieren. Die Verbindung wird danach verschlüsselt und schließlich vom Netz das LOCATION UPDATING ACCEPT gesendet.
Nach derAnmeldung wartet das Mobile entweder auf einen Anruf , oder ist selbst Initiator eines Gesprächs.
Betrachten wir zunächst den Fall, dass das Mobile angerufen wird. Da wir jetzt wissen wie ein CCCH strukturiert ist, können wir davon ausgehen, dass das Mobile den Paging Channel empfängt und verfolgt, ob seine Adresse dort erscheint. Wir werden den stattfindenden Informationsfluss noch genauer verfolgen. Nehmen wir an, das Mobile wird gerufen, es erkennt also seine Adresse in einer Meldung des Paging Channels.
Das Mobile muss jetzt reagieren, dazu muss es als erstes einen Kanal anfordern. Das geschieht auf dem *Random Access Channel* RACH.

Ich muss nun zum Bild 20 ergänzen, dass die dort eingezeichneten Bursts alle Downlink-Kanälen zugeordnet sind. Der Slot 0 der beacon frequency wird uplink allein vom *Random Access Channel* RACH belegt.
Das Mobile sendet zur Kanalanforderung den im Bild 19 dargestellten Accessburst aus. Dieser hat ein auf seine Funktion zugeschnittenes Format. Zunächst hat er nur eine effektive Länge von 88 bit Das ist notwendig, da das Mobile die Entfernung zur BTS nicht kennt. Die Bedeutung dieser Entfernung ergibt sich aus folgender Überlegung:
Die MS oder die BTS Senden und Empfangen abwechselnd, wobei die Filter jeweils umgestimmt werden müssen. Dazu haben beide 3 Burstperioden Zeit. Das Zeitfenster, während dessen die BTS empfängt ist nur so groß, dass ein normaler Burst hineinpasst. Da das Signal eine von der Entfernung abhängige Laufzeit hat, kann es vorkommen, dass ein Burst so spät ankommt, dass ein Teil von ihm schon außerhalb des Fensters liegt. Im praktischen Betrieb wird die Signallaufzeit von der BTS bestimmt und dem Mobile mitgeteilt. Diese (Sende-) Zeitvorverlegung heißt *Timing Advance* TA und kann Werte zwischen 0 und 232 /us annehmen das sind Werte zwischen 0 und 63 bit (eine Einheit = 48/13 /us). Das Mobile muss also um den Wert der TA früher senden.
Ein TA = 0 bedeuted, dass das Mobile nicht mehr als 300 m von der BTS entfernt ist. Desweiteren repräsentiert 1 bit TA-Wert eine Entfernung von 550 m. Als Konsequenz ist ein Mobile das mehr als

300 m + 63 x 550 m = 35 km

von der BTS entfernt ist, nicht mehr erreichbar.
Zum Zeitpunkt der Kanalanforderung auf dem RACH hat sich zwar das Mobile auf den Sender der BTS aufsynchronisiert, sendet aber den Accessburst mit TA=0.
Die 8 Tail Bits am Anfang sind fest kodiert (0011 1010) zusammen mit der Trainingssequenz von 41 Bit weist sie sich gegenüber der BTS als Nutzsignal aus. Die 36 Datenbit enthalten nur 8 Bit Information (yyyxxxxx) . Davon bilden fünf Bit (x) eine Zufallszahl, die es gestattet den Burst von ggf.. , anderen auch eintreffenden zu unterscheiden. In drei Bit (y) ist der Grund der Kanalanforderung verschlüsselt. Solche Gründe sind z.B. „Antwort auf Paging“, „Notruf“, „Nutzer Anforderung“ ...
Die BTS kann aus der Lage des Access Bursts im Empfangfenster den TA berechnen und der MS mitteilen.
In der Meldung IMMEDIATE ASSIGNMENT weist die BTS der MS schließlich einen Arbeitskanal, einen Zeitschlitz, einen logischen Kanal und die genaue Rahmennummer zu, damit die MS mit der BTS Informationen austauschen kann.
Der logische Kanal den die MS zugewiesen bekommt ist ein langsamer zugeordneter Steuerkanal (Slow Dedicated Control Channel) SDCCH.
Bis jetzt hatten wir die Kombination von Tansport-Kanal TCH mit dem langsamen zugeordneten Steuerkanal SACH sowie den allgemeinen Steuerkanal CCCH in den sich BCCH, PACCH, SCH und FCH teilen, besprochen.
Der nunmehr zu betrachtende langsame zugeordnete Steuerkanal (Slow Dedicated Control Channel) SDCCH wird auf dem in Bild 22 gezeigten 102 er Rahmen transportiert.

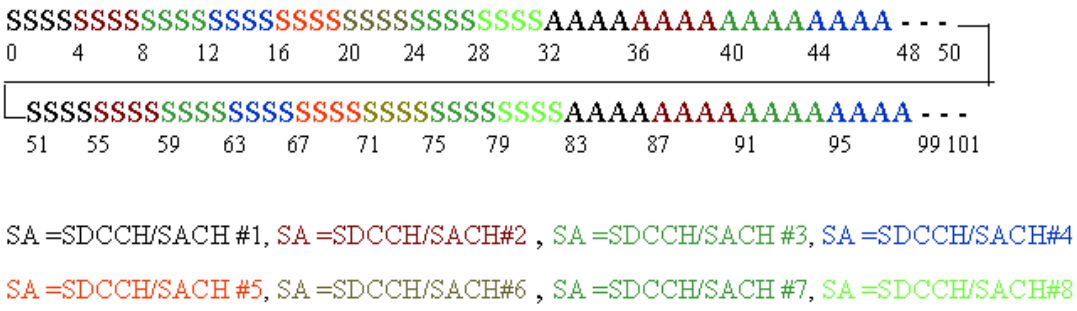


Bild 22: Organisation eines der 8 möglichen SDCCH/SACH/8 Rahmen

Der *Slow Dedicated Control Channel* SDCCH ist (nach Mouly, Pautet [1]) eigentlich ein langsamer Verkehrskanal der für die Signalisation verwendet wird. Betrachten Sie dazu Bild 22. In der dargestellten Zeitorganisation werden im SDCCH/SACH/8 acht Subkanäle unterschieden. Eine Gruppierung in der nur vier Subkanäle existieren ist möglich.

5.7 Die Rolle der Steuerkanäle in einem einfachen Anruf vom ISDN zum GSM

Nachstehend ist ein Ausschnitt aus der Kommunikation zwischen MS und BTS gezeigt, aus dem hervorgeht welche Meldung wann auf welchem logischen Kanal verschickt wird..

A	D	E	F	G	H
1261012	0x03 - LAPD-m	PCH	Down	(RR : PAGING REQUEST TYPE 1)	15 06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B
1261318	0x03 - LAPD-m	PCH	Down	(RR : PAGING REQUEST TYPE 1)	25 06 21 00 05 F4 85 89 1A 31 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B
1261326	0x03 - LAPD-m	RACH	Up	RR CHANNEL REQUEST	
1261328	0x03 - LAPD-m	CCCH	Down	(RR : PAGING REQUEST TYPE 1)	15 06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B
1261332	0x03 - LAPD-m	CCCH	Down	(RR : PAGING REQUEST TYPE 1)	15 06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B
1261338	0x03 - LAPD-m	CCCH	Down	(RR : PAGING REQUEST TYPE 1)	15 06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B
1261342	0x03 - LAPD-m	CCCH	Down	(RR : PAGING REQUEST TYPE 1)	15 06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B
1261349	0x03 - LAPD-m	BCCH	Down	(RR : SYSTEM INFORMATION TYPE 1)	55 06 19 04 00 00 06 00 10 00 00 00 00 00 00 00 00 40 00 A5 00 00 2B
1261359	0x03 - LAPD-m	CCCH	Down	(RR : IMMEDIATE ASSIGNMENT)	2D 06 3F 03 41 40 55 96 BC 26 01 00 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B
1261360	0x03 - LAPD-m	SDCCH	Up	SABM (RR : PAGING RESPONSE)	01 3F 35 06 27 01 03 53 19 81 05 F4 85 89 1A 31
1261379	0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 6)-	03 03 2D 06 1E AA B2 62 F2 10 31 04 55 08 2B 2B 2B 2B 2B 2B 2B
1261449	0x03 - LAPD-m	SDCCH	Down	UA (RR : PAGING RESPONSE)	01 73 35 06 27 01 03 53 19 81 05 F4 85 89 1A 31
1261449	0x03 - LAPD-m	SDCCH	Up	I (RR : CLASSMARK_CHANGE)	01 00 41 06 16 03 53 19 81 20 08 60 14 54 76 15 7B 00 00
1261456	0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1261481	0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 5)	03 03 49 06 1D 10 00 00 00 02 00 00 00 00 00 00 48 20 95 00 00
1261500	0x03 - LAPD-m	SDCCH	Down	I (RR : CLASSMARK ENQUIRY)	03 20 09 06 13 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B
1261500	0x03 - LAPD-m	SDCCH	Up	I (RR : GPRS SUSPENSION REQUEST)	01 22 35 06 34 E7 09 E2 AE 62 F2 10 31 04 01 05
1261551	0x03 - LAPD-m	SDCCH	Down	I (MM : AUTHENTIFICATION REQUEST)	03 42 4D 05 12 01 E0 8C 9A 10 B1 A9 E9 91 5D F2 87 CB 80 B1 17 0D 2B
1261551	0x02 - NAS		Down	MM : AUTHENTIFICATION REQUEST	05 12 01 E0 8C 9A 10 B1 A9 E9 91 5D F2 87 CB 80 B1 17 0D
1261551	0x03 - LAPD-m	SDCCH	Up	I (RR : CLASSMARK_CHANGE)	01 44 41 06 16 03 53 19 81 20 08 60 14 54 76 15 7B 00 00
1261558	0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1261574	0x02 - NAS		Up	MM : AUTHENTIFICATION RESPONSE	05 14 CF A4 B0 53
1261583	0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 6)	03 03 2D 06 1E AA B2 62 F2 10 31 04 D5 08 2B 2B 2B 2B 2B 2B 2B
1261602	0x03 - LAPD-m	SDCCH	Down	RR	01 61 01
1261602	0x03 - LAPD-m	SDCCH	Up	I (MM : AUTHENTIFICATION RESPONSE)	01 46 19 05 14 CF A4 B0 53
1261653	0x03 - LAPD-m	SDCCH	Down	RR	01 81 01
1261660	0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1261685	0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 5)	03 03 49 06 1D 10 00 00 00 02 00 00 00 00 00 00 48 20 95 00 00
1261704	0x03 - LAPD-m	SDCCH	Down	I (RR : CIPHERING MODE COMMAND)	03 84 0D 06 35 01 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B
1261704	0x03 - LAPD-m	SDCCH	Up	RR	03 61 01
1261755	0x03 - LAPD-m	SDCCH	Up	I (RR : CIPHERING MODE COMPLETE)	01 68 09 06 32
1261762	0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 99 19 01 A3 3B 48 09 E3 C2 E9 60 70 52 38 39 5B
1261787	0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 6)	03 03 2D 06 1E AA B2 62 F2 10 31 04 D5 08 2B 2B 2B 2B 2B 2B 2B
1261806	0x03 - LAPD-m	SDCCH	Down	RR	01 A1 01
1261857	0x03 - LAPD-m	SDCCH	Down	I (MM : IDENTITY REQUEST)	03 A6 0D 05 18 02 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B
1261857	0x02 - NAS		Down	MM : IDENTITY REQUEST	05 18 02
1261857	0x03 - LAPD-m	SDCCH	Up	RR	03 81 01
1261857	0x02 - NAS		Up	MM : IDENTITY RESPONSE	05 59 08 3A 85 95 08 80 02 53 04
1261864	0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 9C 1C 01 A1 3B 48 05 D3 C4 F1 65 6C A0 38 51 1C
1261889	0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 5)	03 03 49 06 1D 10 00 00 00 02 00 00 00 00 00 00 48 20 95 00 00
1261908	0x03 - LAPD-m	SDCCH	Down	I (CC : SETUP)	03 A8 4D 13 05 04 01 A0 5C 08 11 81 94 33 57 92 28 F1 7D 02 91 81 2B
1261908	0x02 - NAS		Down	CC : SETUP	13 05 04 01 A0 5C 08 11 81 94 33 57 92 28 F1 7D 02 91 81
1261908	0x03 - LAPD-m	SDCCH	Up	I (MM : IDENTITY RESPONSE)	01 AA 2D 05 59 08 3A 85 95 08 80 02 53 04
1261908	0x02 - NAS		Up	CC : CALL CONFIRMED	93 88 04 06 60 04 02 00 05 81
1261959	0x03 - LAPD-m	SDCCH	Down	RR	01 C1 01
1261959	0x03 - LAPD-m	SDCCH	Up	I (CC : CALL CONFIRMED)	01 AC 29 93 88 04 06 60 04 02 00 05 81
1261966	0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 9F 1F 01 9B 3B 49 05 D4 84 F1 A5 6C A0 38 59 1C
1261991	0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 6)	03 03 2D 06 1E AA B2 62 F2 10 31 04 D5 08 2B 2B 2B 2B 2B 2B 2B
1262010	0x03 - LAPD-m	SDCCH	Down	RR	01 E1 01
1262068	0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 98 18 01 9E 3B 48 05 D5 44 F1 C5 6C 80 38 39 1C
1262093	0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 5)	03 03 49 06 1D 10 00 00 00 02 00 00 00 00 00 00 48 20 95 00 00
1262112	0x03 - LAPD-m	SDCCH	Down	I (RR : ASSIGNMENT COMMAND)	03 EA 31 06 2E 0F 40 55 05 63 41 03 02 28 80 2B 2B 2B 2B 2B 2B 2B
1262112	0x03 - LAPD-m	SDCCH	Up	RR	03 C1 01
1262113	0x03 - LAPD-m	FACCH	Up	SABM	01 3F 01
1262145	0x03 - LAPD-m	FACCH	Up	SABM	01 3F 01
1262176	0x03 - LAPD-m	FACCH	Down	UA	01 73 01
1262176	0x03 - LAPD-m	FACCH	Up	I (RR : ASSIGNMENT COMPLETE)	01 00 0D 06 29 00
1262176	0x02 - NAS		Up	CC : ALERTING	93 C1
1262207	0x03 - LAPD-m	FACCH	Down	RR	01 21 01
1262207	0x03 - LAPD-m	FACCH	Up	I (CC : ALERTING)	01 02 09 93 C1
1262229	0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 5)	03 03 49 06 1D 10 00 00 00 02 00 00 00 00 00 00 48 20 95 00 00
1262237	0x03 - LAPD-m	FACCH	Down	RR	01 41 01
1262241	0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 DB 1B 01 9E 3B 44 05 D5 44 F1 45 6C 50 38 29 1C
1262333	0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 5)	03 03 49 06 1D 10 00 00 00 02 00 00 00 00 00 00 48 20 95 00 00
1262345	0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 DE 1E 01 9D 3B 48 89 E2 C2 E9 25 6C 40 38 19 1C
1262437	0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 6)	03 03 2D 06 1E AA B2 62 F2 10 31 04 D5 08 2B 2B 2B 2B 2B 2B 2B

Bild 23: Ausschnitt aus dem EXCEL-Arbeitsblat eines Mobile Terminated Call (MTC)

Das obige Bild zeigt einen mit dem Programm *OT Drive 4* exportierten Trace. In den Spalten sind folgende Werte bzw. Bezeichnungen aufgeführt:

Spalte A: Eine Zeitmarke, die die Anzahl der seit Beginn des Einschaltens des Mobile empfangenen TDMA-Rahmen wiedergibt. Ein TDMA-Rahmen hat die Länge 120/26 = 4,615 ms.
Spalte D: Kennzahl aus dem „Message log ..“ für die nachstehende Bezeichnung des TraceStrings Spalte M. Es bedeuten:
- LAPD-m (Link Access Protokoll D-Kanal –mobile). Das sind Nachrichten der Schicht 2.
- NAS (Non Access Stratum) Das sind Nachrichten die nicht zu den Radio Ressoure Meldungen (zu Access Stratum) gehören. (Stratum -> Layer)

Spalte E: Logischer Kanal auf dem die Meldung transportiert wird. Vergl. Die Bilder 21 und 22
Spalte F: Richtung der Übertragung.
Spalte G: Protokoll Discriminator, RR = Radio Ressource Messages, MM = Moblity Management Messages, gefolgt vom Name der Meldung. Die Klammer bedeutet, dass der Meldung eine Oktett Pseudolänge vorangestellt ist. SABM bedeuted dass eine gesichterte Verbindung angefordert wird . I bedeuted, dass der Schicht 2 Rahmem nummeriert ist. Nur RR bedeutet die reine Schicht 2 Nachricht Receiver Ready.
Spalte M: Tracestring.
Der Inhalt der einzelnen Meldungen wird später ausführlich erklärt. Es wurde ein einfacher Anruf aus dem ISDN an das Trace-Mobile im Netz des Operators D1 mitgeschnitten. Der Rohtrace wurde mit OT Drive 4 exportiert und das EXCEL - File mit Namen *LM.csv* in ein EXCEL - Arbeitsblatt mit Namen *MTC*.xls importiert und formatiert . Man erkennt, dass in Bild 23 zwei Arbeitsblätter montiert wurden.
Solange das Mobile im *idle mode* arbeitet ist der Hintergrund des Arbeitsblattes weiß. Tauscht das Mobile mit der BTS auf einem gesichterten Kanal Steuerinformationen aus, ist der Hintergrund hellgelb gefärbt. An der Zeitmarke 1262112 sendet das Netz in der Meldung ASSIGNMENT COMMAND die Nummer des Transportkanals. Daraufhin beantragt das Mobile mit dem Rahmen 1262113 (SABME) erneut den „acknowledged mode“ (Quittungsbetrieb).. Vom Netz im Rahmen Nummer 1262176 mit UA bestätigt.
Die Kanalanforderung ist rot markiert , die zum Trace gehörende Zahl 96 ist leider der Formatierung zum Opfer gefallen.
Dem Arbeitsheft [5] ist eine CD beigefügt. Sie enthält einen vollständige MTC-Trace, der mt einem OT 260 aufgenommen wurde Nach dem Autostart der CD, klickt man auf die Schaltfläche „Rohtrace“ und in der erscheinenden Powerpoint-Folie auf den Titel „Anruf aus dem ISDN in das D1-Mobilfunknetz“.

In Bild 23 kann nun leicht abgelesen werden welche Kanäle im idle mode (weißer Hintergrund) aktiv sind. Vor der Zuweisung des Transportkanals werden Sicherheitschecks durgeführt, das geschieht in dem gelb markierte Bereich auf dem SDCCH. Der MEASUREMENT REPORT wird grundsätzlich auf dem SACCH transportiert.
Wenn der Transportkanal zugewiesen ist erfolgt die Steuerung nur noch über den SACCH und dem FACCH.

Die Zuweisung der Kanäle geschieht durch die Meldungen IMMEDIATE ASSIGNMENT und ASSIGMENT COMMAND

.

5.8 Über die Fehlersicherung im GSM Übertragungskanal

Ein kompletter Layer 2 Rahmen besteht , außer beim CHANNEL REQUEST, bei dem wir ja wissen, dass er nur aus acht Bit besteht, immer aus 23 Oktetten.
Einem Rahmen der nicht genug relevante Oktette besitzt werden Restoktette der Gestalt „2B“ hinzugefügt.
Fehler im Signalkanal zwischen MS und BTS dürfen nicht nur erkannt, sondern müssen sofort korrigiert werden. Der Fehlerkorrektur dient ein FireCode bei dem das Nutzsignal der Länge 23 x 8 = 184 bit mit dem Polynom $(X^{23}+1)(X^{17}+X^3+1)$ multipliziert wird. Dadurch erhöht sich die Länge des zu übertragenden Rahmen auf 224 bit. Es lässt sich theoretisch beweisen, dass damit Bündelfehler bis zum Gewicht 11 korrigiert werden können.
Das Prinzip der Fehlerkorrektur soll nachstehend phänomenologisch erklärt werden:
Multipliziert man alle mögliche Kombinationen der 184 bit des L2-Rahmens mit dem o.g. Polynom. Dann bekommen Sie die gleiche Anzahl (2^{183}) Polynome oder nennen wir sie Kodeworte, die aber nun die Länge 224 besitzen. Polynome der Länge 224 gibt es aber 2^{223} Stück.
Wenn nun eines der 2^{183} Kodeworte der Länge 224 beschädigt wird, das darf an 11 Bitpositionen sein, so stimmt es natürlich mit keinem der 2^{183} Kodeworte die aus den 184 bit des L2-Rahmens hervorgegangen sind überein Überprüft man jedoch das gestörte Polynom mit den möglichen ungestörten auf Ähnlichkeit. So ist das Bitmuster des gestörte Wortes dem Bitmuster des Original immer noch ähnlicher als seinem Nachbarn.
Das heist,das gestörte Polynom unterscheidet sich in weniger Stellen vom Original als von jedem anderen möglichen Kodewort.
Nun besteht jedoch die Möglichkeit, dass der kodierte L2-Rahmen von einer Bündelstörung getroffen wird die mehr als 11 Fehler erzeugt.
Daher kodiert daher noch einmal mit einem sogenannten Faltungskode. Dadurch werden die 228 bit langen Kodevektoren auf die doppelte Länge d.h. auf 456 Bit gespreizt. Grob gesagt ist dadurch zwischen zwei Nutzbits ein Füllbit untergebracht. Wenn also ein Störburst (also eine Kette von Störbits) auftritt, treffen sicher einige Störbit auf Füllbits und sind dadurch wirkungslos.

Damit man nach der Spreizung auf 8x57 bit kommt, werden an die 224 bit nach der Fire-Kodierung einfach 4 bit angehängt sehen Sie dazu Bild 20. Danach wird der auf 456 bit gespreizte Rahmen durch 4 Bursts übertragen.

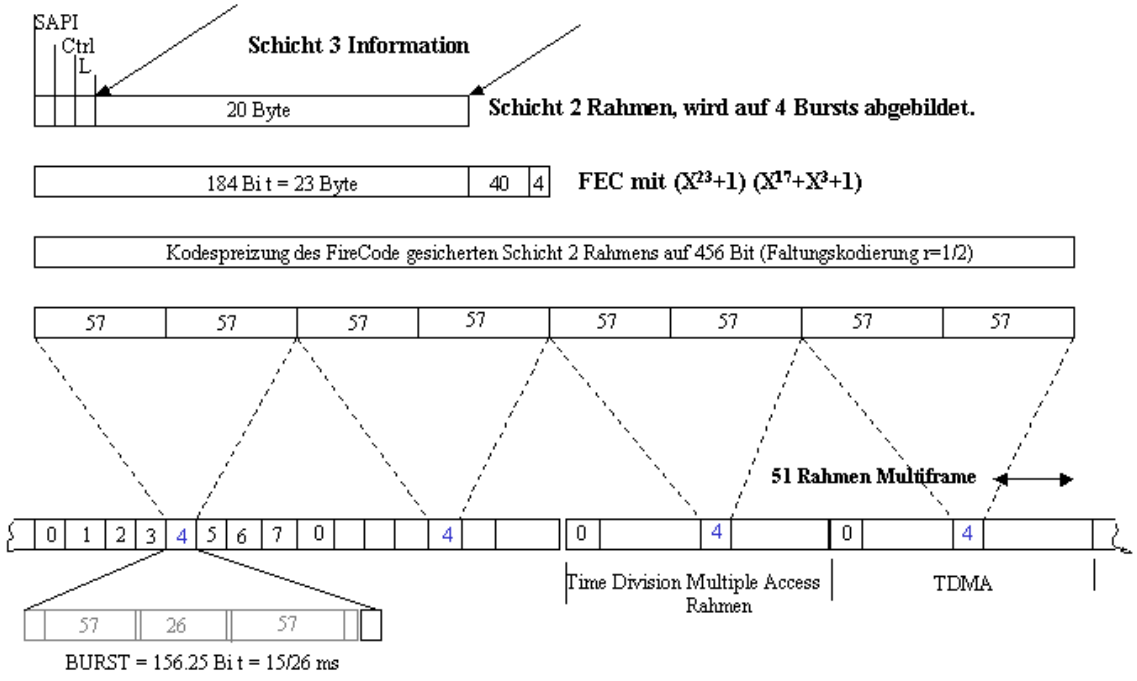


Bild 24: Abbildung eines Schicht 2 Rahmens auf die Schicht 1

6. Die Schichten 2 und 3 im GSM

6.1 Über die Schicht2

Im Zusammenhang mit Bild 13 hatten wir zwei Verschiedene Typen von Meldungen kennengelernt.
Meldungen die zum Non Access Stratum (NAS) gehören und Meldungen die mit dem Link Access Protokoll-mobile (LAPD-m) gesichert sind. Im Bild 13 waren aus Gründen der Platzersparnis die Radio Resource (RR) messages nicht enthalten. Diese muss man in konsequenter Weiterführung der Terminologie zum Access Stratum (AS) rechnenn
Die ersten beiden Rahmen im Bild 25 sind dem LAPD-m Typ zuzuordnen, der dritte (Schicht 3 Rahmen) kann entweder den NAS oder dem AS zugeordnet werden, je nach dem Prokoll-diskriminator. Das soll aber weiter unten besprochen werden.

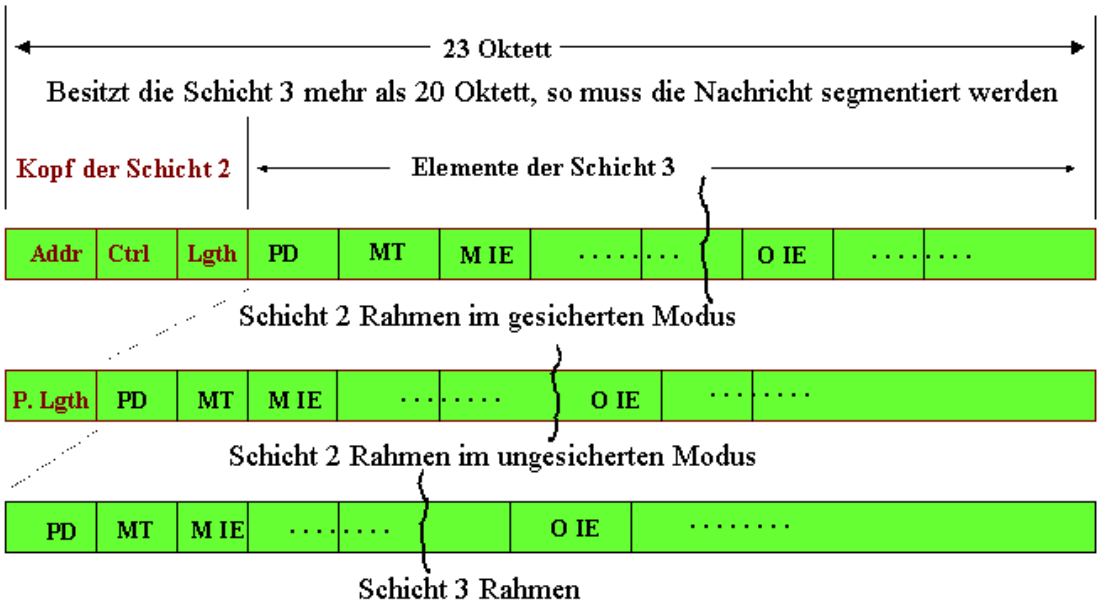


Bild 25: Der Aufbau von Meldungs Rahmen auf der Luftschnittstelle

Im Bild 25 sehen Sie einen Rahmen im gesicherten Modus (Acknowledged mode). Er erinnert an den Aufbau eines L2-Rahmens im ISDN. Wie noch zu erklären ist, stehen für Adresse und Steuerung jeweils nur ein Oktett zur Verfügung.
Wie im Zusammenhang mit dem Rahmenaufbau der MSU im SS#7 erklärt habe gibt es hier Pflicht-Informationselemente (M IE) und Optionale Informationselemente (O IE) .
Im ungesicherten Mode ist in der Schicht 2 dem Layer 3 Rahmen nur ein Oktett die *Pseudo- Länge* vorangestellt. Der Aufbau der Informationselemente, die Pseudolänge stellt ein Informationselement dar, ist in Bild 26 dargestellt.

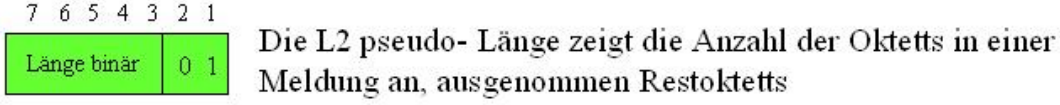


Bild 26: Definition der Pseudolänge und Typen von Informations Elementen

Wie aus Bild 26 hervorgeht, muss man bei der Umrechnung der Pseudolänge in Dezimalwerte den Hexadezimalwert zunächst als Binärzahl darstellen muss, sodann sind die beiden bit mit den niedrigsten Werten zu streichen. Danach kann die Länge berechnet werden .

Zum Begriff Restoktett:
Wie aus Bild 24 hervorgeht, geht man bei der Kodierung der Informationen zur Fehlersicherung davon aus, dass ein Rahmen eine Länge von 23 Oktett hat. Längere L3 Rahmen werden segmentiert, kürzere werden mit Oktetts der Gestalt „2B“ aufgefüllt.
Die Oktetts der Gestalt „2B“ können nicht grundsätzlich unberücksichtigt bleiben. Es gibt nämlich Meldungen, in den die Restoktette in die Informationsübertragung einbezogen werden.. Wir werden uns bei deren Auftreten, später im Text, näher damit beschäftigen.

Bezüglich des Aufbaus des Kopfes der Schicht 2 in Bild 25, betrachten wir nun die Darstellung in Bild 27. Im Adressfeld fehlt, im Vergleich mit dem ISDN, der TEI, weil wir es bei der Luftschnittstelle mit einer Punkt zu Punkt Verbindung zu tun haben. Der Raum für die Nummerierung für den SAPI ist auf drei bit begrenzt. Das C/R bit entspricht dem im ISDN, das EA-bit ist 1, weil kein weiteres Adressoktett folgt.
Der SAPI = 0 steht für Signalisierung in Call Control, Mobility Management und Radio Resource Management, während der SAPI = 3 in SMS Meldungen angewandt wird.

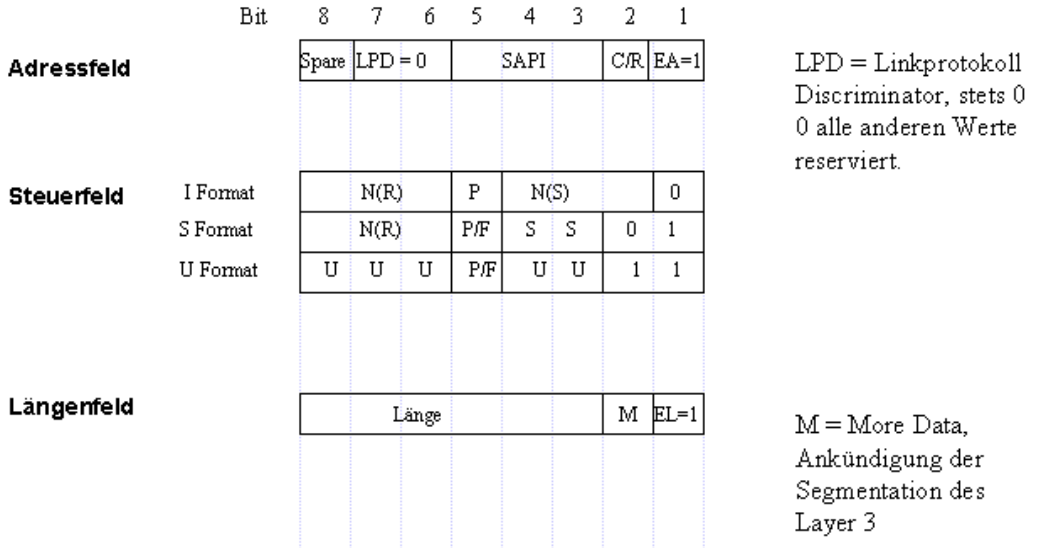


Bild 27: Aufbau des Kopfes einer Schicht 2 Nachricht

Die Nummerierung in den Steuerfeldern entspricht weitestgehend denen im ISDN. Da im GSM nur drei bit für N(S) und N(R) zur Verfügung stehen wird auf der Luftschnittstelle modulo 8 gezählt. Kodierung der Supervisory-Kommandos und die der Unnummerierten Kommandos entspricht der aus dem ISDN bekannten.
Die Codierungen von bit 1 und 2 im Längenfeld, entsprechen der in der Pseudolängenangabe.
Das More Data bit wird gesetzt, wenn die Schicht 3 Nachricht segmentiert werden muss. Für Leser die nicht mehr so stark mit den Termini im ISDN vertraut sind, sollen noch einmal die in Bild 28 benutzten Abkürzungen erklärt werden. Es bedeuten:
N(R) : Die Nummer des erwarteten Blocks modulo 8
N(S) : Die Nummer des gesendeten Blocks modulo 8
P : Poll-Bit, es wird sofortige Antwort erwartet.
F : Final-Bit Antwort auf Nachricht mit gesetztem Pollbit
RR : Receiver Ready, empfangene Nachricht in Ordnung, Empfänger bereit zum Empfang

RNR : Receiver not Ready, empfangene Nachricht nicht in Ordnung, Empfänger nicht bereit
REJ : Reject, Nachricht ist nicht auswertbar, wird zurückgewiesen.
SABM : Set Up Asynchronous Balanced Mode, Antrag auf Übergang in den Quittungsbetrieb.
UA : Unnumered Acknowledge, Bestätigung von SABME oder DISC.
DM : Disconnect Mode, Nachricht ist nicht aauswertbar
UI : Unnumbered Information, keine Quittung der übertragenen Information erforderlich
DISC : Disconnect, Abbau des Quittungsbetriebs.

Format	Kommando	Antwort	8 7 6	5	4 3 2	1
Information	I		N(R)	P	N(S)	0
Supervisory	RR	RR	N(R)	P/F	0 0	0 1
	RNR	RNR	N(R)	P/F	0 1	0 1
	REJ	REJ	N(R)	P/F	1 0	0 1
Unnumbered	SABM		0 0 1	P	1 1	1 1
		DM	0 0 0	F	1 1	1 1
	UI		0 0 0	P	0 0	1 1
	DISC		0 1 0	P	0 0	1 1
		UA	0 1 1	F	0 0	1 1

Bild 28: Kodierung der Steuerungskommandos und -Antworten im L2 Rahmen

6.2 Über die Schicht3

Der Aufbau des Schicht 3 Rahmens geht im Detail aus Bild 29 hervor. Das erste Oktett enthält (wie im ISDN) den *Protocol Discriminator* PD. Im ISDN folgt dem PD die *Call Reference* CR. Diese heißt hier *Transaction Identifier* und ist mit dem *Protocol Discriminator* in einem Oktett untergebracht. Das *Flag* F zeigt (wie im ISDN das bit Nr. 8 des Wertes der CR an, wer den TI festgelegt hat.

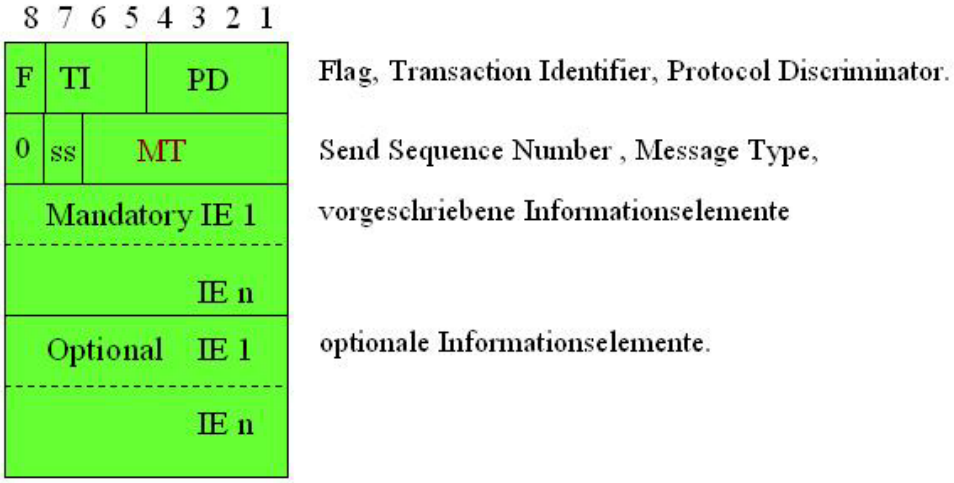


Bild 29: Auf eines Rahmens der Schicht 3

Die im GSM üblichen Protocol Discriminatoren sind in Tafel 8 dargestellt

0011 **C**all **C**ontrol und Rufabhängige **SS** Meldungen
0101 **M**obility **M**anagement Meldungen (nicht GPRS)
0110 **R**adio **R**esource Management Meldungen
1001 SMS Meldungen
1011 Rufunabhängige **S**uplementary **S**ervice Meldungen

Tafel 6: Protokolldiskriminatoren

Die Bedeutung von Flag und Transaction Identifier entsprechen denen der Callreference im ISDN:
Flag = 0 es sendet die Seite die den TI festlegt
Flag = 1 es empfängt die Seite die den TI festlegt

Im zweiten Oktett des Schicht 3 Rahmens ist das 8. Bit immer 0. Das Bit Nummer 7 ist die *Send Sequence Number*, es wird inkrementiert, wenn eine Meldung ein zweites mal gesendet wird, ehe die erste Meldung quittiert ist. So können die beiden Meldungen unterschieden werden.
Danach folgen die Oktette mit den Informationselementen die in der Meldung enthalten sein müssen (Mandatory IE) und die in der Meldung enthalten sein können (Optionale IE).
Im Sinne konsequenter Reduzierung der Belastung von Übertragungswegen, existieren die in Tafel 7 dargestellten Kombinationen von Typ, Länge und Wert.
So kann ein optionals IE vom Format T sein. Z.B. muss in einer SETUP Meldung nur der Titel des IE CLIR Invocation vorhanden sein, damit das Netz weiß, dass der Nutzer die Unterdrückung seiner Rufnummer wünscht.
Ist es andererseits Pflicht ein Informationselement mit in der Recommendation festgelegter Länge an einer bestimmten Stelle der Meldung zu übertragen, so kann man sowohl Längenangabe als auch Titel weglassen.
Bei einem optionalen IE genau definierter Länge genügt die Angabe des Titels und des Wertes.
Es gibt Pflichtelemente deren Länge und Wert vom Status der Übertragung abhängen. Sie sind folglich vom Format LV.
Optionale Elemente können auch unterschlidliche Länge und Werte besitzen.

Format	**Bedeutung**	**IEI vorh.**	**Länge vorh.**	**Wert vorhanden**
T	Typ allein	ja	nein	nein
V	Wert allein	nein	nein	ja
TV	Typ und Wert	ja	nein	ja
LV	Länge und Wert	nein	ja	ja
TLV	Typ, Länge und Wert	ja	ja	ja

Tafel 7: In den ETS angewandte Bezeichnung für Informationselemente

.

7. Die Meldungen für das Radio Resource Management

Betrachten wir als erstes die Meldungen die wir aus dem Arbeitsblatt MTC in Bild 23 kennen „ Anruf aus dem ISDN in das D1-Mobilfunknetz“ kennen. Anschließend schauen wir uns an, welche Nachrichten ausgetauscht werden wenn sich das Mobile am Netz anmeldet.

7.1 Die Meldung PAGING REQUEST 1

Bitte Betrachten Sie in Bild 23 den Rahmen Nummer 1261318. Es ist eine Meldung vom Typ LAPD-m, d.h. eine Layer 2 Nachricht. Der Layer 2 Rahmen besitzt als Kopf eine Pseudolength 25_H d.h. der Schicht 3 Rahmen besitzt die Länge 9. im Mobile wird diese Schicht 2 Nachricht auf die Schicht 3 hochgereicht. In Tafel 8 finden Sie die Übersetzung der Schicht 3 Nachricht Wie bereits gesagt wurden aus Platz-gründen im Bild 23 die RR-Messages ausfiltert. Die Meldung wird entsprechen Table 9.22/GSM 04.08 übersetzt. Entsprechend der Terminologie von Tafel 7 folgen dem Message Typ 21 zwei Pflichtelement vom Format V und der fest gelegten Länge = ½ . Es sind dies Page Mode und Channel Needed. Es folgt das Pflichtelement Mobile Identity 1 vom Format LV.

Table 9.22/GSM 04.08 lässt noch ein optionale Informationselement Mobile Identity 2 vom Format TLV zu. Bei starkem Verkehr könnte mit der genannten Meldung noch ein zweites Mobile gerufen werden. Aus Gründen der Geheimhaltung wird das Mobile nicht mit seiner IMSI gerufen, sondern mit einer temporären IMSI der sog. TMSI die das Mobile bein Einbuchen ins Netz erhält und die regelmäßig geändert wird.

```
_____[ 463 ]___[ 1261318 ]___[ DOWN ]___[ RR ]_____________

06 21 00 05  f4 85 89 1a  31 2b 2b 2b  2b 2b 2b 2b  2b 2b 2b 2b
2b 2b

06  ----0110  Protocol Discrim.   : radio resource management messages

21  00100001  MESSAGE TYPE        : PAGING REQUEST TYPE 1

00  ----00--  spare bits          : 0
    ------00  Page Mode           : Normal paging
    --00----  Channel Needed      : (first) Any Channel
    00------  Channel Needed      : (second) Any Channel

: Mobile Identity 1
05  00000101  length of Mob.ident.: 5
f4  1111----  Identity Digit 1    : hex value = f, if  TMSI/P-TMSI
    ----0---  No. of ID digits    : even
    -----100  Type of identity    : TMSI/P-TMSI
85  10000101  Identity Digit 2,3  : take hex value
89  10001001  Identity Digit 4,5  : take hex value
1a  00011010  Identity Digit 6,7  : take hex value
31  00110001  Identity Digit 8,9  : take hex value
```

Tafel 8 : Die Meldung PAGING REQUEST TYPE !

7.2 Die Meldung SYSTEM INFORMATION TYPE 1

Im *idle mode* muss das Mobile nicht nur die Paging Informationen abhören um festzustellen wann es gerufen wird, sonder auch noch sämtliche Informationen über das System in das es sich eingebucht hat, dazu gehören eine ganze Reihe von Kennziffern und Werten, die die im Folgenden erklärt wereden. Beginnen wir mit der SYSTEM INFORMATION TYPE 1. In Bild 23 erscheint eine solche Meldung mit der Zeitmarke 1261349. In dieser Meldung wird mitgeteilt über welche Knäle die BTS verfügt. Dieser Vorgang heißt *Cell Allocation* CA (Zell Zuteilung).

```
_____[ 452 ]___[ 1261349 ]___[ DOWN ]___[ RR ]_____________

06 19 04 00  00 06 00 10  00 00 00 00  00 00 00 00  40 00 a5 00
00 2b

06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages

19  00011001  MESSAGE TYPE         : SYSTEM INFORMATION TYPE 1

: Cell Channel Description
04  00------  Format Type          : Bit Map 0 format
    --00----  2 spare bits         : 0
    -----1--  Cell Allocation      : ARFCN 123
06  -----1--  Cell Allocation      : ARFCN 99
    ------1-  Cell Allocation      : ARFCN 98
10  ---1----  Cell Allocation      : ARFCN 85
40  -1------  Cell Allocation      : ARFCN 15

: RACH Control Parameters
a5  10------  Max. of retransmiss  : 4
    --1001--  slots  to spread TX  : 12
    ------0-  The cell is barred   : no
    -------1  Call reestabl.i.cell : not allowed

00  00000---  Acc. contr. cl. 11-15: 0 The cell is not barred,,1 The cell is barred,.
    -----0--  Emergency Call EC 10 : allowed
    ------00  Acc. contr. cl.  8-9 : 0 The cell is not barred,,1 The cell is barred,.

00  00000000  Acc. contr. cl. 0-7  : 0 The cell is not barred,,1 The cell is barred,.
```

Tafel 9: Übersetzung einer Meldung SYSTEMINFORMATION TYPE 1

Außerdem wird im Abschnitt *RACH Control Paramerts* festgelegt auf welche Weise der Zugriff zum Netz organisiert wird.
Wenn ein Mobile mit dem Netz Verbindungen aufnehmen will, so sendet es bekanntermaßen auf dem RACH einen Access Burst. Da andere Mobiles zur gleichen Zeit ebenfalls Access Burst senden können besteht die Gefahr der Kollision Das Mobile wird, falls der Access Burst unbeantwortet bleibt, einen weiteren Zugriffsversuch starten. Da das an der Kollision beteiligt Mobile ebenfalls einen weiteren Access Burst senden wird, bestellt die Gefahr einer nochmaligen Kollision. Damit das nicht passiert, wird jedem Mobile eine Zufallszahl „Tx“ von zwischen 3 und 50 (Zeitschlitzen) zugewiesen, nach denen ein weiterer Zugriffsversuch zum Netz erfolgen darf.
Außerdem wird festgelegt wie oft (Max. of retransmissions) ein Zugriffsversuch wiederholt werden darf.
Weitere Festlegungen die das Zugriffsverhalten regeln sind Angaben über eine evtl. Sperre der Zelle (cell is barred), und ob bei einem Verbindungsverlust in der Zelle (z.B. durch plötzliches Auftreten eines Hindernisses) in der gleichen Zelle die Verbindung wieder aufgebaut werden darf (Call reestablishment). Beides wird im Beispiel verneint.

Es existier ein Mechanismus mit dem bei starkem Verkehr der Zugriff zur Funkzelle geregelt werden kann. Man unterscheidet die Benutzerklassen 0...15. Allen Nutzerklassen kann bei Netzüberlastung der Zugriff zum Netz zeitweilig verweigert werden.
Die Nutzerklasse 10 ist der Notruf. In dieser Klasse sowie in den Klassen 11 bis 15 (Not- und Sicherheitsdiensten sowie Techniker des Netzwerkes) darf ggf. noch auf das Netz zugegriffen werden , wenn es für gewöhnliche Nutzer schon gesperrt ist

Es ist festgelegt, dass diese Zugriffsberechtigungen 4 mal in der Sekunde ausgestrahlt werden , d.h. dass diese Information in allen BCCH Meldungen ausgestrahlt wird.

7.3 Die Meldung SYSTEM INFORMATION TYPE 2

In der SYSTEM INFORMATION TYPE 2 (Tafel 10) werden die Frequenzen der BCCH in den Nachbarzellen und der *Network Colour Code* NCC des Operators übergeben.

```
_____[ 577 ]___[ 1256096 ]___[ DOWN ]___[ RR ]_____________

06 1a 00 00  00 00 02 10  00 00 00 00  00 48 20 95  00 00 08 a5
00 00

06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages

1a  00011010  MESSAGE TYPE       : SYSTEM INFORMATION TYPE 2


00  00------  bitmap 0 format
    --0-----  Extension Indicator : The IE carries the complete BA
    ---0----  BCCH alloc. sequ.num: 0

02  ------1-  BCCH alloc. RF chan.: 90
10  ---1----  BCCH alloc. RF chan.: 85
48  -1------  BCCH alloc. RF chan.: 39
    ----1---  BCCH alloc. RF chan.: 36
20  --1-----  BCCH alloc. RF chan.: 30
95  1-------  BCCH alloc. RF chan.: 24
    ---1----  BCCH alloc. RF chan.: 21
    -----1--  BCCH alloc. RF chan.: 19
    -------1  BCCH alloc. RF chan.: 17

08  ----1---  BCCH carrier with NCC = 3 is permitted for monitoring;

a5  10------  Max. of retransmiss.: 4
    --1001--  12 slots used to spread TX
    ------0-  The cell is barred  : no
    -------1  Call reestablishment in cell is not allowed

00  -----0--  Emergency Call EC 10: allowed
    00000---  acc ctrl class 11-15: 0/1 access permitted/forbidden
    ------00  acc ctrl class  8-9 : 0/1 access permitted/forbidden

00  00000000  acc ctrl class  0-7 : 0/1 access permitted/forbidden

00  00000000  acc ctrl class  0-7 : 0/1 access permitted/forbidden
```

Tafel 10: Inhalt einer Meldung SYSTEM INFORMATION TYPE 2

In Bild ist eine solche Systeminformation nocht enthalten, sie liegt außerhalb des dargestellten Bereichs.

7.4 Die Meldung SYSTEM INFORMATION TYPE 3

Betrachten wir die SYSTEM INFORMATION TYPE 3 (Tafel 11). Sie ist etwas umfangreicher wie die bisher besprochenen. Damit der Leser die Erkläungen im Text besser den Zeilen im Text zuordnen kann, sind Textstellen und Tracezeilen gleichermaßen markiertt.

```
_____[ 507 ]___[ 1256351 ]___[ DOWN ]___[ RR ]_____________

06 1b aa b2  62 f2 10 31  04 d8 04 3c  55 65 04 a5  00 00 3e 33 2b 2b

06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages

1b  00011011  MESSAGE TYPE       : SYSTEM INFORMATION TYPE 3
```

```
: Cell Identity
aa  10101010  Cell identity value1: Hex-Wert verwenden
b2  10110010  Cell identity value2: Hex-Wert verwenden
: Location Area Identification
62  ----0010  Mobile CC digit 1   : 2
    0110----  Mobile CC digit 2   : 6
f2  ----0010  Mobile CC digit 3   : 2
    1111----  Mobile NC digit 3   : 15
10  ----0000  Mobile NC digit 1   : 0
    0001----  Mobile NC digit 2   : 1

31  00110001  Loc. area code (LAC) = ID of MSC (hex)
04  00000100  Loc. area code (LAC) = ID of BSC (hex)

: Control Channel Description
d8  1-------  MSC is Release '99 onwards
    -1------  MSs in the cell shall apply IMSI attach and detach procedure
    --011---  Number of blocks    : 3 reserved for access grant
    -----000  1 basic physical channel used for CCCH not combined with SDCCHs
04  0-------  spare
: Cell Bar Qualify 3
    -00-----  Iu mode not supported
    ---00---  spare
: BS-PA-MFRMS
    -----100  6 multi fr. period for transm. PAGING REQUEST mesgs. to the same paging subgroup
3c  00111100  T3212 TimeOut value : 60 deci hours

: Cell Options BCCH,
55  0-------  1 spare bit         : 0
    -1------  PWRC Power control indicator is set
    --01----  MSs shall use uplink discontinous transmission
    ----0101  Radio Link Timeout  : 24

: Cell Selection Parameters;
65  011-----  Cell Resel. Hyster. : 6 dB RXLEV hysteresis for level average (LA) re-selection
    ---00101  Max Tx power level  : Mobile may use 5
04  0-------  Addition. Reselect Param ind: in SI4 rest octets, i.p., SI7, SI8 rest octets, ..
    -0------  New establishment cause is not supported
    --000100  RXLEV ACCESS MIN    : -110 +4 db permitted

: RACH  Control Parameters
a5  10------  Max. of retransm.   : 4
    --1001--  used to spread TX   : 12 slots
    ------0-  The cell is barred  : no
    -------1  Call reestablishment in cell is not allowed
00  -----0--  Emergency Call EC10 : allowed
    00000---  Acc.contr.cl. 11-15 : 0/1 access permitted/forbidden
    ------00  Acc.contr.cl.   8-9 : 0/1 access permitted/forbidden
00  00000000  Acc.contr.cl.   0-7 : 0/1 access permitted/forbidden

: SI 3 Restoktett
          0  Selection Parameters not present
          0  Power Offset  not present
          1  System Information 2ter Indicator not available
          1  Early Classmark Sending Control is allowed
          1  Scheduling if and where not present
          1  GPRS indicator = present
: RA COLOUR
        100  Routing Area colour = 4
: SI13 Position
          0  SYSTEM INFORMATION TYPE 13 message is sent on BCCH Norm;
: 3G early Classmark Sending Restriction
          1  Neither UTRAN, CDMA2000 nor GERAN IU MODE CLASSMARK CHANGE message shall be sent
: SI2quater_POSITION
          1  SYSTEM INFORMATION TYPE 2 quater message is sent on BCCH Norm .
: End SI 3 Restoktett
```

Tafel 11: Inhalt einer Meldung SYSTEM INFORMATION TYPE 3

Die ersten beiden Zeilen sind die eindeutige Nummer der Zelle des D1-Netzes .
Die *Location Area Identification* besteht aus dem Ländercode (CC) für Deutschland (262) und dem Netzwerkcode (NC) für D1 (01) .
Der Bezeichnung nach stellen die nächsten beiden Zeilen die Nummer der Vermittlung (MSC 31) und die Nummer der Basisstation (BSC 04) in diesem Vermittlungsbereich dar.

Gehen wir zeilenweise vor und beginnen mit dem ersten Oktett der Control Channel Description
d8 hex :

- das Mobile Switching Center besitzt.mindesten den Ausgabestand 1999
- In der Zelle wird IMSI attach/detach angewendet. Dieser etwas eigenartige Begriff bedeutet lediglich, dass sich das Mobile im VLR (durch Ein- und Ausschalten) an und abmeldet, damit ein ausgeschaltetes Mobile nicht unnötig gesucht wird.
- Gibt an wie viele der Paging Kanäle im Rahmen für Access Grant (Zugriffsgewährung) verwendet werden
- Im CCCH werden keine Zeitschlitze für einen SDCCH reserviert. Das entspricht somit der Darstellung auf Bild 17 .

04 hex:

- damit das Mobile nicht ständig das Paging abhören und damit Strom verbrauchen muss, hat man den sog. Diskontinuierlichen Empfang (DRX) eingeführt. Abgeleitet von der IMSI des Teilnehmers wird dem Mobile eine Paging (Unter-)Gruppe zugewiesen. In unserem Beispiel dauert es 6 Multiframe- Perioden bis die Paging Gruppe des Mobiles wieder ausgesendet wird, das Mobile also in den Kanal hineinhören muss.

3c hex:

- Der Timer 3212 bestimmt, nach wie viel Stunden sich das eingeschaltete Mobile, wenn es z.B. ruhig auf dem Tisch liegt, im Netz melden muss. Der Vorgang wird auch als Periodische Aktualisierung des Standortes (*Periodic Location Updating*) bezeichnet.

Das nächste Oktett beschreibt Optionen der Zelle des BCCH:

- PWRC bedeutet, dass die Leistung der aktiven MS geregelt wird
- Das Mobile wird angewiesen Uplink zur Diskontinuierlichen Übertragung DTX überzugehen.

Im Interesse einer langen Batteriestandzeit werden im Mobilfunk alle Möglichkeiten des Energiesparens eingesetzt. Eine davon ist die diskontinuierliche Übertragung. Man geht davon aus, dass bei Sprachübertragung längere Sprachpausen auftreten. In diesen Zeiten könnte man den Sender ausschalten. Da das Abschalten des Senders beim Hörer den Eindruck der Unterbrechung der Verbindung hinterlassen würde wird in den Gesprächspausen ein sog. Komfortgeräusch (*comfort noise*) erzeugt und Übertragen. Die Energieeinsparung besteht darin, dass im aktiven Gespräch ein Rahmen mit 260 bit aller 20ms ausgesendet wird, in den Gesprächspausen wird ein solcher Rahmen aller 480 ms übertragen.
Radio Link Timeout bedeutet, wenn eine GSM-Verbindung in einer aktiven Phase abbricht, z.B. wenn der Nutzer mit seinem Fahrzeug in eine Tiefgarage einfährt, so muss es eine Möglichkeiten geben den Zustand des Abbruchs zu definieren. Das geschieht durch Zählen der nicht dekodierbaren SACH-Rahmen durch die BTS. Diese Anzahl ist hier mit 24 festgelegt.

Das Kriterium nachdem die optimale Funkverbindung bestimmt wird heißt ***C1***. In die Berechnung von ***C1*** gehen folgende Größen ein:

- Der Mittelwert des empfangenen Pegels = M
- Der Wert *p1=RXLEV_ACCESS_MIN*, das ist der Minimalpegel mit dem diese BTS von einer MS empfangen werden muss um als Serving Cell in Frage zu kommen. (-106 dBm)
- Der Wert *p2=MX_TXPWR_MAX_CCH,* ist die maximale Sendeleistung die ein Mobile auf dem RACH ausstrahlen darf sie liegt zwischen 13 dBm und 43 dBm.
- Der maximalen Sendeleistung der Mobilstation. = P

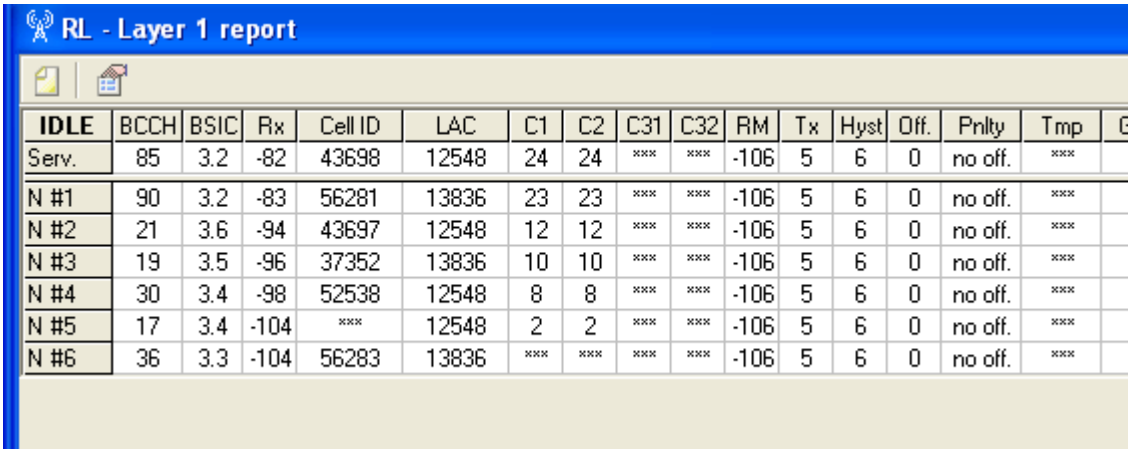
Die maximale Sendeleistung einer MS ist von der Leistungsklasse (*Power class*) abhängig. In der ETS 05.05 ist für GSM 900 festgelegt:

Power class	:	1	2	3	4	5
Nominal max. output power:		(20 W)	8 W (39 dBm)	5 W (37dBm)	2 W (33 dBm)	0,8 W (29 dBm)

Wie in den *Cell Selection Parameters* zu lesen ist, wird dem Mobile der maximal Leistungs-Ausgangspegel 5, d.h. 0,8 W (29 dBm) vorgeschrieben.

Mit den oben genannten Größen gilt $C1 := (M\text{-}p1) - Max.((p2 - P),0)$.

Betrachten wir den *Layer 1 Report* den wir mit einem SAGEM Trace Mobile und dem Programm *OTDrive4* erzeugen können.. In der ersten Spalte sind die aktuelle und die Nachbarzellen eingetragen, in der 6. Spalte steht der *C1* Werte. Sechs Spalten daneben stehen die Werte für die *Cell Reselect Hysterese.*



IDLE	BCCH	BSIC	Rx	Cell ID	LAC	C1	C2	C31	C32	RM	Tx	Hyst	Off.	Pnlty	Tmp
Serv.	85	3.2	-82	43698	12548	24	24	***	***	-106	5	6	0	no off.	***
N #1	90	3.2	-83	56281	13836	23	23	***	***	-106	5	6	0	no off.	***
N #2	21	3.6	-94	43697	12548	12	12	***	***	-106	5	6	0	no off.	***
N #3	19	3.5	-96	37352	13836	10	10	***	***	-106	5	6	0	no off.	***
N #4	30	3.4	-98	52538	12548	8	8	***	***	-106	5	6	0	no off.	***
N #5	17	3.4	-104	***	12548	2	2	***	***	-106	5	6	0	no off.	***
N #6	36	3.3	-104	56283	13836	***	***	***	***	-106	5	6	0	no off.	***

Bild 29: Layer 1 Report eines SAGEM Trace Mobiles

Die Bedeutung der Cell Reselect Hysterese besteht darin dass auf der Grenze zwischen zwei Zellen oftmals die C1-Werte beider Zellen nahezu gleich sind. Einmal ist die eine größer, wenige Meter weiter die andere. Damit nicht laufend ein Umbuchen (Hand over) in eine andere Zelle statt findet weist man dem *C1*-Wert der Zelle in dem sich das Mobile gerade befindet einen Beharrungsfaktor, diese *Cell Reselect Hysterese* zu (hier 6 dBm).

Der Wert *RXLEV_ ACCESS_ MIN* stellt den schwächsten Pegel dar, bei dem auf eine BTS noch zugegriffen werden darf, er beträgt 106 dBm.

Die *RACH Control Parameters* wurden bereits erklärt,

Das SI 3 Restoktett ist nach der CSN.1 bitweise kodiert. Mouly bezeichnet CSN.1 als *Concrete Syntax Notation 1*. Es wird auch die Bezeichnung *Compact Syntax Notation* 1 verwendet. Entsprechend Table 9.32/GSM 04.08 ist das Informationselement SI 3 Rest Octets ein Pflichtelement vom Format V und der Länge 4 Die vier Oktetts sind gemäß Tafel 13 „3e 33 2b 2b"
Die Decodierung der Restoktetts erfolgt bitweise. Das Kriterium für die Auswertung sind nicht die Bitwerte 0 und 1 , sondern L (low) und H (high) . Um im vorliegenden Fall L und H zu berechnen, wird die Bitfolge der 4 Restoktette (3e 33 2b 2b) mit der Bitfolge der Oktette 2b 2b 2b 2b modulo 2 addiert und 0 = L , 1 = H gesetzt. Man erhält:

LLLHLHLH LLLHHLLL LLLLLLLL LLLLLLLL

Die Werte L und H können nun in die Anweisungen ETSI TS 144 018 V6.16.0 Table 10.5.2.34.1 Eingesetzt werden. Das sieht so aus:

<SI3 Rest Octet> ::= <Optional selection parameters>
<Optional Power offset>
<System Information 2ter Indicator>
<Early Classmark Sending Control>
. .....

<Optional Selection Parameters> ::= **L** | **H** <Selection Parameters>;
<Optional Power Offset> ::= **L** | **H** <**Power Offset**: bit (2)>;

System Information 2ter Indicator (1 bit field)
L SYSTEM INFORMATION TYPE 2ter message is not available
H SYSTEM INFORMATION TYPE 2ter message is available
Early Classmark Sending Control (1 bit field)
L Early Classmark Sending is forbidden
H Early Classmark Sending is allowed

Aus der oben stehenden Berechnung erhält man in Tafel 13:

```
: SI 3 Restoktett
           0  Selection Parameters not present
           0  Power Offset  not present
           1  System Information 2ter Indicator not available
           1  Early Classmark Sending Control is allowed
              ............
```

Tafel 12: Übersetzung von SI 13 Restoktett

Für die in Tafel 12 angedeutete Berechnung der Werte des SI 13 Restoktetts sind also nicht die Binärdigits der Hexzahlen des Tracestrings entscheident, sonder die L und H Werte die aus der modulo 2 Addition der Restoktette mit 2b entstehen.

7.5 Die Meldung SYSTEM INFORMATION TYPE 4

Die Meldung SYSTEM INFORMATION TYPE 4 (Tafel 13) enthält offensichtlich Elemente die schon in den SYS_INFO_1...3 übertragen wurden. Dazu kommt ein Restoktett, welches GPRS Eigenschaften des Kanals betrifft, weshalb es übergangen werden soll.

```
_____[ 493 ]___[ 1256811 ]___[ DOWN ]___[ RR ]_____________

06 1c 62 f2  10 31 04 65  04 a5 00 00  11 2b 2b 2b  2b 2b 2b 2b
2b 2b

06  ----0110  Protocol Discrim.   : radio resource management messages

1c  00011100  MESSAGE TYPE        : SYSTEM INFORMATION TYPE 4

: Location Area Identification
62  ----0010  Mobile CC digit 1   : 2
    0110----  Mobile CC digit 2   : 6
f2  ----0010  Mobile CC digit 3   : 2

    1111----  Mobile NC digit 3   : 15
10  ----0000  Mobile NC digit 1   : 0
    0001----  Mobile NC digit 2   : 1

31  00110001  Loc. area code (LAI), ID of MSC (hex)
04  00000100  Loc. area code (LAI), ID of BSC (hex)

: Cell Selection Parameters
65  011-----  Cell Reselect Hyst. : 6 dB RXLEV hyst. For LA re-select
    ---00101  Max Tx power level  : MS may use 5

04  0-------  No Additional cells in SysInfo 7-8
    -0------  New establishm.cause: not supported
    --000100  RXLEV ACCESS MIN permitted = -110+4dB

: RACH Control Parameters
a5  10------  Max. of retransmissions
    --1001--  12 slots used to spread TX
    ------0-  The cell is barred  : no
    -------1  Call reestab.in cell: not allowed

00  -----0--  Emergency Call EC 10: allowed
```

```
    00000---  Acc. ctrl class11-15: bit pattern,0 = access permitted, 1 = access forbidden
    ------00  Acc. ctrl class 8-9 : bit pattern,0 = access permitted, 1 = access forbidden
00  00000000  Acc. ctrl class 0-7 : bit pattern,0 = access permitted, 1 = access forbidden

: SI4 Rest Octets
: SI4 Rest Octets_O
: Optional  selection parameters
          0  Selection Parameters = not present
: End Optional  selection parameters
: Optional Power offset
          0  Power Offset = not present
: End Optional Power offset
: GPRS Indicator
          0  High: GPRS indicator = present
: RA COLOUR
        100  Routing Area colour = 4
: SI13 Position
          0  SYSTEM INFORMATION TYPE 13 message is sent on BCCH Norm;
: End GPRS Indicator
: End SI4 Rest Octets_O
: Break Indicator
          1  High Additional parameters, "SI4 Rest Octets_S" are sent in SYSTEM INFORMATION
TYPE 7 and 8
: End SI4 Restoctet
```

Tafel 13: Inhalt einer Meldung SYSTEM INFORMATION TYPE 4

7.6 Die Meldung SYSTEM INFORMATION TYPE 5

Entsprechend Bild 23 findet man die SYSTEM INFORMATIONEN 1 bis 4 in den weiß hinterlegten Feldern und die SYSTEM INFORMATIONEN 5 und 6 in den farbig hinterlegten Feldern.
Die SYSTEM INFORMATIONEN 1 bis 4 werden nur im *idle mode* ausgestrahlt.

```
_____[ 298 ]___[ 1263997 ]___[ DOWN ]___[ RR ]_____________

06 1d 10 00  00 00 02 00  00 00 00 00  00 48 20 95  00 00

06  ----0110  Protocol Discrim.   : radio resource management messages

1d  00011101  MESSAGE TYPE        : SYSTEM INFORMATION TYPE 5

10  00------  Format Type         : Bit Map 0 format
    --0-----  Extension Indicator : The IE carries the complete BA
    ---1----  BCCH allocation sequence number indication 1

02  ------1-  BCCH alloc. RF chan.: 90
48  -1------  BCCH alloc. RF chan.: 39
    ----1---  BCCH alloc. RF chan.: 36
20  --1-----  BCCH alloc. RF chan.: 30
95  1-------  BCCH alloc. RF chan.: 24
    ---1----  BCCH alloc. RF chan.: 21
    -----1--  BCCH alloc. RF chan.: 19
    -------1  BCCH alloc. RF chan.: 17
```

Tafel 14: Inhalt einer Meldung SYSTEM INFORMATION TYPE 5

Im dedicated mode kann sich Standort des Mobiles ändern, folglich muss dem Mobile mitgeteilt werden in welche Nachbarzellen es sich ggf. einbuchen kann. In der SYSTEM INFORMATION TYPE 5 (Tafel 14) sind die Kanalnummern dieser BCCH aufgeführt.
Das Mobile führt auf diesen Kanälen ständig Messungen aus und meldet die Messergebnisse an das Netz.

7.7 Die Meldung SYSTEM INFORMATION TYPE 6

Mit der Meldung SYSTEM INFORMATION TYPE 6 (Tafel 15) wird dem Mobile laufend mitgeteilt wo es sich befindet. Die Informationen die hie übergeben werden wurden bereits besproche.

```
_____[ 302 ]___[ 1263893 ]___[ DOWN ]___[ RR ]_____________

06 1e aa b2  62 f2 10 31  04 d5 08 2b  2b 2b 2b 2b  2b 2b

06  ----0110  Protocol Discrim.   : radio resource management messages

1e  00011110  MESSAGE TYPE        : SYSTEM INFORMATION TYPE 6


: Cell Identity
aa  10101010  Cell identity value1, Hex Wert
b2  10110010  Cell identity value2, Hex Wert

: Location Area Identification
62  ----0010  MCC digit 1         : 2
    0110----  MCC digit 2         : 6
f2  ----0010  MCC digit 3         : 2

    1111----  MNC digit 3         : 15
10  ----0000  MNC digit 1         : 0
    0001----  MNC digit 2         : 1

31  00110001  Location area code (LAI), Number of MSC
04  00000100  Location area code (LAI), Number of BSC

: Cell Options (SACH)
d5  -1------  Power control indic.: is set
    --01----  MSs shall use uplink discont.transmission
    ----0101  Radio Link Timeout  : 24

: NCC Permitted
08  ----1---  BCCH carrier with NCC = 3 is permitted for monitoring;
```

Tafel 15: Inhalt einer Meldung SYSTEM INFORMATION TYPE 6

7.8 Die Meldung CHANNEL REQUEST

Nach der Besprechung der System Informationen die in einem MTC vorkommen, soll nun mit der Erklärung der Meldungen chronologisch zum Bild 19 forgefahren werden

Das Mobile beantwortet den Paging Request mit einer Kanalanforderung auf dem Random Access Channel. Die Meldung CHANNEL REQUEST (Tafel 16) ist nur 8 bit lang. Von diesen 8 bit sind mindestens 3 bit der Grund für die Kanalanforderung. Die übrigen 5 bit werden von einer Zufallsfolge gebildet, die dazu dient den Urheber der Kanalanforderung zu markieren.
Typische Gründe für die Kanalanforderung sind:

Emergency call	(Notruf)	101
Answer to paging	(Antwort auf Paging)	100
Originating call…	(Rufaufbau)	111
Call reestablishing..	(Ruf Wiederaufbau)	110
Location Updating	(Standort Aktualisierung)	000

usw.

```
_____[ 462 ]___[ 1261326 ]___[ UP ]___[ LAPDm ]_____________

96

L2-RACH Channel Request

96  100-----  Answer to paging, Any Channel requested
```

Tafel 16: Inhalt einer Meldung CHANNEL REQUEST

Damit mehr Gründe spezifiziert werden können, dürfen für den Grund der Kanalanforderung bis zu 6 bit verwendet werden. Die Zufallsfolge darf dann nur noch 5 bis 2 bit in Anspruch nehmen.

7.9 Die Meldung IMMEDIATE ASSIGNMENT

In Beantwortung desChannel request weist das Netz dem Mobile einen Kanal zu, auf dem als erstes eine Dienstverbindung aufgebaut werden muss. Das geschieht mit der Meldung IMMEDIATE ASSIGNMENT (Tafel 17) Es wird der Kanal 85, der schon in der SYSTEM INFORMATION 1 angekündigt wurde als Dienstkanal zugewiesen, dazu der Zeitschlitz Nummer 1 und eine Timing Advance von 1 bit.
Der logische Kanal ist ein *SDCCH/SACH/8*, den wir im Zusammenhang mit Bild 22 besprochen hatten. Zugewiesen wird der Subkanal 0 (das entspricht im Bild 22 dem Subkanal 1) .

Im IE *Request Reference* wird auf den Inhalt der Kanalanforderung verwiesen und auf die Zufallszahl in der Meldung Channelrequest.
Der etwas eigenartige Ausdruck *same as before* im Halboktett *Page Mode* steht anstelle des üblichen „reserviert für zukünftigen Gebrauch“. Damit wird den Netzbetreibern die Möglichkeit gegeben diesem Begriff eine eigene Bedeutung zuzuordnen.
Im Halboktett *Dedicated Mode or TBF* ist angezeigt dass hier ein Kanal fest zugewiesen wird, im Gegensatz zum GRPS bei dem auf einem Kanal nur zeitweilig Pakete übertragen werden .

Von großer Bedeutung ist die Zuweisung der aktuellen Rahmennummer die durch Zuweisung der drei Werte T1, T2 und T3 erfolgt. Es gilt:

$$FN \text{ modulo } 42432 = 51x((T3-T2) \textit{mod}\ 26)+T3+51x26xT1' , \quad \text{mit } T1' = T\ 1 \textit{ mod } 32$$

```
_____[ 450 ]___[ 1261359 ]___[ DOWN ]___[ RR ]_____________

06 3f 03 41  40 55 96 bc  26 01 00 2b  2b 2b 2b 2b  2b 2b 2b 2b
2b 2b

06  ----0110  Protocol Discrim.   : radio resource management messages

3f  0-------  1 spare bit         : 0
    -0------  Send sequence number: 0

    --111111  MESSAGE TYPE        : IMMEDIATE ASSIGNMENT

: Page Mode
03  ----00--  2 spare bits        : 0
    ------11  Page mode           : same as before
: Dedicated Mode or TBF
    0-------  1 spare bit         : 0
    -0------  Two messages assign.: No meaning
    --0-----  Downlink assig to MS: No meaning
    ---0----  This message assigns a dedicated mode resource

: Channel Description
41  01000---  Ch.type & TDMA offs.: SDCCH/8 + SACCH/C8|CBCH(SDCCH/8),SubChannel 0
    -----001  Timslot number      : 1
```

```
: Schalter
40  010-----  Training sequ. code : 2
    ---000--  Single channel      : RF single channel
    ------00  Singl.RF ch.high prt: 0
55  01010101  abs.RFch.num.low prt: 85

: Request Reference
96  100-----  Establishing Cause  : Answer to paging
    ---10110  Random Reference    : 22

: Rahmennummer
       10111  23      = (T1)     is coded as the bin. Repr. of (FrameNumber div 1326) mod 32.
      100001  33      = (T3)     is coded as the binary representation of FrameNumber mod 51.
       00110  6       = (T2)     is coded as the binary representation of FrameNumber mod 26.
: The frame number, FN modulo 42432 can be calculated as 51x((T3-T2)mod 26)+T3+51x26xT1'

: Timing Advance
01  00------  2 spare bits         : 0
    --000001  Timing advance value : 1 bit period

: Mobile Allocation
00  00000000  length=0
```

Tafel 17: Inhalt einer Meldung IMMEDIATE ASSIGNMENT bei Frequenzsprung

7.10 Die Meldung PAGING RESPONSE

Wie aus Bild 23 zu ersehen ist, beginnt mit der Meldung PAGING RESPONSE der *acknowledged mode* auf dem Kanal. Das ist notwendig um den Einfluss von Störungen auf die Verhandlung über die Kanalparameter weitgehend auszuschließen. In Tafel 18 ist daher nicht die Layer 3 Message sondern der in die Schicht 2 eingebettete Rahmen der Meldung PAGING RESPONSE dargestellt.
Die Meldung enthält vier Informationselemente.

(1) Die Ciphering Key Sequence Number, die wie im Abschnitt 7.10.1 gezeigt eine Information über den Schlüssel enthält.

(2) Dazu gehört (in der Recommendation als IE bezeichnet) ein leeres halbes Oktett.

(3) Das Informationselement *Mobile Station Classmark 2* meldet dem Netz Informationen über die technischen Eigenschaften und Möglichkeuten des Mobiles.

- Da sich diese technischen Möglichkeiten während des Betriebes ändern können, muss die Möglichkeit bestehen die Classmark dynamisch während des Betriebs zu ändern.
- Die möglichen Verschlüsselungsalgorithmen werden gemeldet,
- sowie die Leistung des Mobiles
- Es wird die Möglichkeit des SMS Empfangs gemeldet, sowie
- die Frequenzbänder auf denen das Mobile kommunizieren kann

(4) Die Mobile Identity wurde im Zusammenhang mit der Meldung Paging Request besprochen.

```
_____[ 448 ]___[ 1261360 ]___[ UP ]___[ LAPDm ]_____________

01 3f 35 06  27 01 03 53  19 81 05 f4  85 89 1a 31

01  0-------  Spare               : 0
    -00-----  Link Prot. Disc.    : 0
    ---000--  SAPI                : 0
    ------0-  C/R Flag            : 0, MS side to BS side
    -------1  EA                  : 1
3f  00111111  Unnumbered          : SABM                      P=1
35  001101--  length              : 13
    ------0-  M                   : 0
    -------1  EL                  : 1
```

```
06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages

27  0-------  1 spare bit         : 0
    -0------  Send sequence number: value
    --100111  MESSAGE TYPE        : PAGING RESPONSE

: Ciphering Key Sequence  Number
01  ----0---  1 spare bit         : 0
    -----001  Ciph. key sequ. num.: 1 (7=no key available)
    0000----  4 spare bits        : 0

: Mobile Station Classmark 2
03  00000011  lgth of MS Cl.Mark2 : 3

53  0-------  1 spare             : 0
    ---1----  "Controlled Early Classmark Sending" option is implemented in the MS
    ----0---  Encryp.Algor. A5_1  : available
    -----011  RF power capability : Class 4, handheld

19  0-------  1 spare bit         : 0
    -0------  pseudo-synch.capab. : not present
    --01----  SS Screening Indic. : phase 2 error handling
    ----1---  Mobile station supports mobile terminated point to point SMS
    -----0--  no VoiceBroadcastService (VBS) capability or no notifications wanted
    ------0-  no VoiceGroupCallService (VGCS) capability or no notifications wanted
    -------1  The MS does support the E-GSM or R-GSM

81  -0------  1 spare bit         : 0
    --0-----  LocationServiceValueAdded Capability  not supported
    ---0----  1 spare bit         : 0
    ----0---  SoLSA Capability    : not supported
    -----0--  Network initiated MO CM connection request not supported.
    ------0-  encryp.algorith.A5/3: not available
    -------1  encryp.algorith.A5/2: available

: Mobile Identity

05  00000101  length of Mob. ident: 5
f4  1111----  Identity Digit 1    : 15
    ----0---  No. of ID digits    : even
    -----100  Type of identity    : TMSI/P-TMSI
85  10000101  Identity Digit 2,3  : take hex value
89  10001001  Identity Digit 4,5  : take hex value
1a  00011010  Identity Digit 6,7  : take hex value
31  00110001  Identity Digit 8,9  : take hex value
```

Tafel 18: Inhalt einer Meldung PAGING RESPONSE

7.10.1 Über die Verschlüsselung des Transportkanals

Das erste Informationselement in der Meldung PAGING RESPONSE war *Ciphering key Sequence Number.* Zu dessen Erklärung ist es notwendig näher auf die Verschlüsselung im GSM einzugehen. Eine absolut sichere Methode der Verschlüsselung besteht darin einen binär codierten Text (plain text) mit einer (echten) Zufallsfolge über einen *Modulo 2 Addierer* zu verknüpfen. Dann lässt sich nämlich theoretisch nachweisen, dass die Summe (der Geheimtext) wieder ein absolut zufällige Folge ist, also für einen Fremden, der die Zufallsfolge (den Schlüssel) nicht kennt nicht entschlüsselbar ist.
Kennt man auf der Seite des Empfängers die Zufallsfolge, ist es möglich durch *Modulo 2 Addition* mit dem Verschlüsselten Text den offenen Text wieder zu erzeugen.

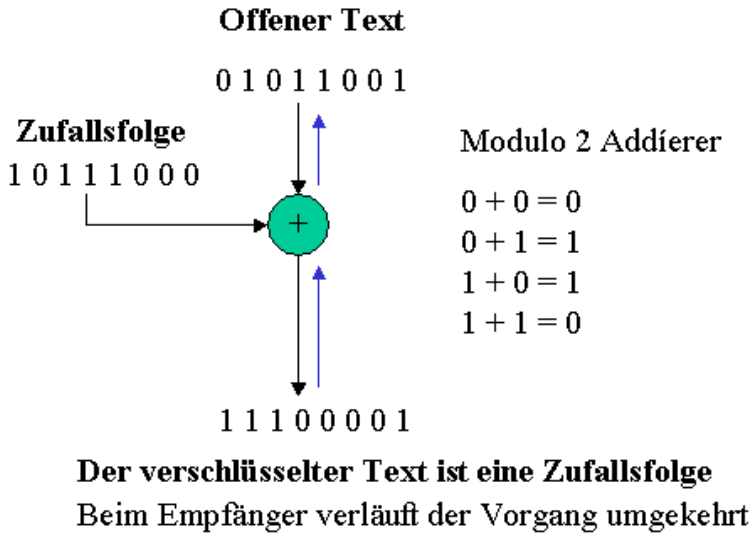


Bild 30: Das Prinzip einer Verschlüsselung

Eine solche Zufallsfolge ließe sich zum Beispiel durch eine radioaktive Quelle erzeugen. Das Problem besteht nur darin, dass beim Empfänger, synchron zum Sender, die gleiche Quelle existieren muss. Das gezeigte Beispiel bleibt also ein Gedankenexperiment. In der Praxis bedarf es komplizierter mathematischer Überlegungen um eine Quasi-Zufallsfolge zu erzeugen, bzw. den Plain Text so umzuformen, dass das Ergebnis einer Addition mit einer echten Zufallsfolge sehr nahe kommt. Im Mobilfunk verwendet man das in Bild 31 dargestellte Verfahren

.

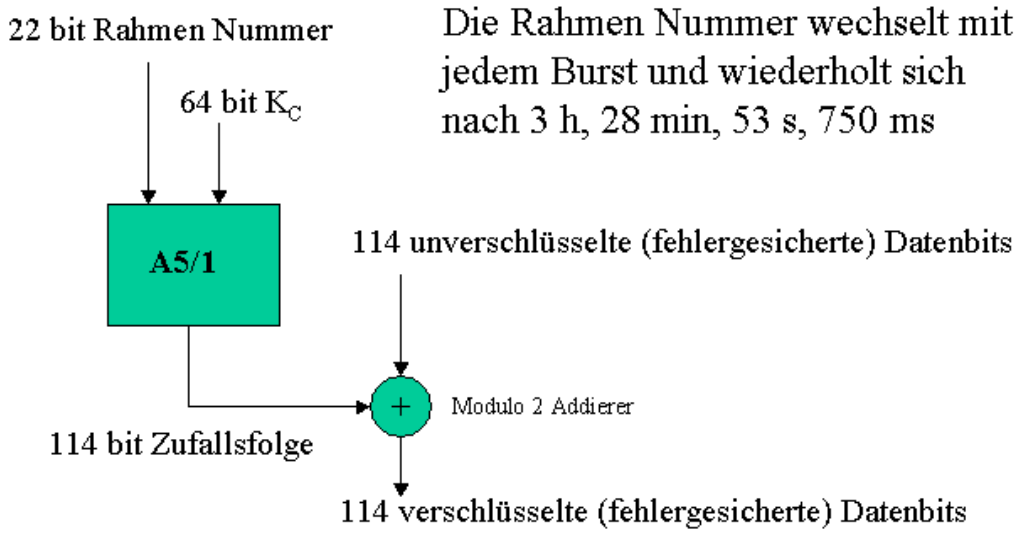


Bild 31: Verschlüsseln im Mobilfunk

Mit Hilfe eines Verschlüsselungsalgorithmus mit Namen A5/X (X=1..5) der im Mobile und im Netz zur Verfügung steht, wird die sich zyklisch ändernde Rahmennummer mit einer 64 bit langen Quasi-Zufallszahl Kc zu einer 114 bit langen Verschlüsselungs- Sequenz verknüpft.
Diese Sequenz wird mit dem entsprechend Bild 20 erzeugten 114 bit langen Nutzinformationen eines Bursts modulo 2 verknüpft.

Was die Periode der Rahmennummer von 3 Stunden, 28 Minuten, 53 Sekunden und 750 Millisekunden betrifft, so erinnern Sie sich bitte an die Darstellung auf Bild 13 in der dargestellt wird wie diese Periode zustande kommt.

Die Zahl Kc steht, wie man auf Bild 3 ablesen kann, auf der SIM-Karte des Mobiles. Sie wird nach der im Bild 28 dargestellten Methode verzeugt..
Die dem Schlüssel Kc zugeordnete. *Ciphering Key Sequenz Number* CKSN, als *Kc number* bezeichnet) ist mit ersterem genauso im Netz bekannt. Die CKSN wird allein verwendet um dem Netz mitzuteilen welcher Schlüssel Kc im Mobile gespeichert ist. Die CKSN wird bei der Anmeldung des Mobiles im Netz (in der Meldung LOKATION UPDATE REQUEST) und in der Meldung PAGING RESPONSE übertragen.

Mit der nachstehenden Methode wird erreicht, dass sowohl Mobile als auch Netz über die gleiche Kc samt CKSN verfügen

Betrachten Sie dazu Bild 32. Sie kennen sicherlich das Prinzip der Parole, wobei ein Wachtposten einer sich nähernden Person die Frage nach dem Losungswort stellt. Er ruft „Parole!“ und der sich nähernde muss die (geheime) Antwort sagen.

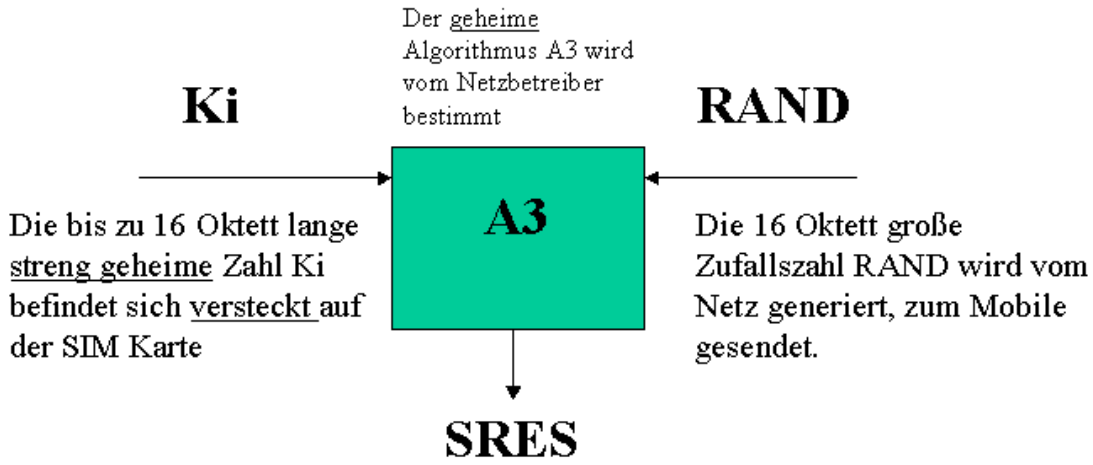


Bild 32: Die Erzeugung einer „Parole“ (SRES)

Im Mobilfunk wir die Authentifizierung (z.B. während der Anmeldung des Mobiles beim Netz, dem *Location Update*) dadurch eingeleitet, dass das Netz die Meldung AUTHENTICATION REQUEST (Tafel 19) zum Mobile sendet (Frage nach der Parole).
In dieser Meldung wir eine 16 Oktett lange Zufallszahl, genannt RAND (von random, zufällig) übergeben Diese Zahl wird aus 2^{128}-1 Möglichkeiten ausgewählt!!.
In der Meldung AUTHENTICATION RESPONSE (Tafel 20) wird die Antwort in Gestalt des (Signet RESULT) SRES übergeben.
SRES ist eine 4 Byte lange Zahl, die mittels des (streng) geheimen, von jedem Operator (Netzbetreiber) getrennt festgelegten Algorithmus A3 und dem (streng) geheimen bis zu 16 Byte langen Zahl Ki , berechnet wird. Ki ist auf der SIM-KARTE (für Unbefugte nicht lesbar) untergebracht. Der Schlüssel Ki ist jedem Nutzer individuell zugeteilt und mit anderen Daten im HLR gespeichert.
Das Netz berechnet SRES nach der gleichen Methode und vergleich mit diesem Wert die Antwort des Mobiles. Stimmen die Werte überein, gilt das Mobile als authentifiziert.

```
_____[ 432 ]___[ 1261551 ]___[ DOWN ]___[ NAS ]_____________

05 12 01 e0  8c 9a 10 b1  a9 e9 91 5d  f2 87 cb 80  b1 17 0d

05  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0101  Protocol Discrim.   : mobility management messages non GPRS
12  00------  SendSequenceNumber  : 0

    --010010  MESSAGE TYPE        : AUTHENTICATION REQUEST

01  0000----  Spare
    ----0---  Spare
    -----001  Ciph.Key Seq. Numb. : 1

: Authentication parameter RAND
e0  11100000  Parameter 1         : 224
8c  10001100  Parameter 2         : 140
9a  10011010  Parameter 3         : 154
10  00010000  Parameter 4         : 16
b1  10110001  Parameter 5         : 177
a9  10101001  Parameter 6         : 169
e9  11101001  Parameter 7         : 233
91  10010001  Parameter 8         : 145
5d  01011101  Parameter 9         : 93
f2  11110010  Parameter 10        : 242
87  10000111  Parameter 11        : 135
cb  11001011  Parameter 12        : 203
80  10000000  Parameter 13        : 128
b1  10110001  Parameter 14        : 177
17  00010111  Parameter 15        : 23
0d  00001101  Parameter 16        : 13
```

Tafel 19: Inhalt einer Meldung AUTHENTIKATION REQUEST

```
_____[ 428 ]___[ 1261574 ]___[ UP ]___[ NAS ]_____________

05 14 cf a4  b0 53

05  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0101  Protocol Discrim.   : mobility management messages non GPRS
14  00------  SendSequenceNumber  : 0

    --010100  MESSAGE TYPE        : AUTHENTICATION RESPONSE

: Authentication Parameter SRES
cf  11001111  Parameter 1         : 207
a4  10100100  Parameter 2         : 164
b0  10110000  Parameter 3         : 176
53  01010011  Parameter 4         : 83
```

Tafel 20: Inhalt einer Meldung AUTHENTIKATION RESPONSE

Gleichzeitig mit der Berechnung von SRES wird in Netz und Mobile der Schlüssel Kc erzeugt, zusammen mit einer 3 bit langen *Ciphering Key Sequence Number* CKSN. Das erfolgt ähnlich der Erzeugung von SRES (siehe Bild 28) unter Verwendung von Ki und RAND jedoch mit dem Algorithmus A8. Im Kommando PAGING RESPONSE (Tafel 18) wird diese CKSN zum Netz übertragen und damit festgelegt welcher Schlüssel Kc zu verwenden ist.

Es existieren nun zwei Kc, einen der schon auf der SIM-Karte enthalten war und dessen CKSN beim Anmelden bereits übertragen wurde und einen der im Zuge der Authentifizierung erzeugt wurde.

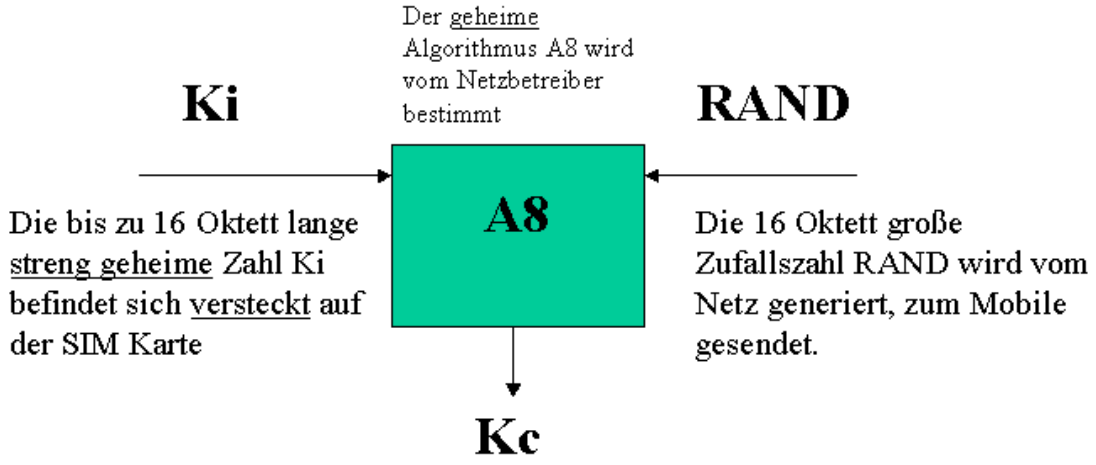


Bild 33: Die Erzeugung des Schlüssels Kc

Der aktuell erzeugte Schlüssel Kc ist damit ein Reserveschlüssel, der genauso im Netz gespeichert ist, und der über seinen CKSN in Dienst gestellt werden kann.

7.10.2 Das IE Mobile Station Classmark 2

Mit dem Begriff *Classmark* werden die technischen Eigenschaften eines Mobiles bezeichnet, auf die sich das Netz während einer Mobile-Verbindung einstellen muss. In der Meldung PAGING RESPONSE werden die hauptsächlichen technischen Eigenschaften im IE Mobile Station Classmark 2 vorab gemeldet. Eine umfassendere Meldung dieser Art erfolgt in der Meldung CLASSMARK CHANGE (Abschnitt 7.11) oft ausgelöst von der Meldung CLASSMARK ENQUIRY.

- Da haben wir zunächst den Softwarestand (Revision Level), der, da die ETS Vorschriften ständig fortgeschrieben werden, für Kompatibilitätsbetrachtungen erforderlich ist.
- Der etwas eigenartige Begriff *Early classmark sending* bedeutet, dass das Mobile nachdem es die Meldung CLASSMARK CHANGE vom Netz empfangen hat, so bald wie möglich zusätzliche Angaben zur technischen Ausstattung liefert.
- Das Mobile meldet sodann über welchen Verschlüsselungsalgorithmus (hier A5/1) es verfügt
- Sodann wird die Leistungsklasse des Mobiles (hier 2 Watt) gemeldet.
- Im nächsten Oktett wird gemeldet, dass das Mobile beim Handover den Timing Advance Wert nicht abschätzen kann. (pseudo-synchronization capability)
- Der SS-Screening Indicator bezieht sich auf Eigenschaften der vom Mobile beherrschten Dienstmerkmale (Suplementary Services)
- Das Mobile kann SMS senden und empfangen
- Sprach-Broadcast und -Gruppenrufdienste unterstützt das Mobile nicht.
- Es wird E-GSM oder R-GSM unterstützt.

LocationServiceValueAdded Capability not supported bedeuted dass das Leistungsmerkmal den Aufenthaltsort des Mobiles zu bestimmen nicht zur Verfügung steht.

.

7.11 Die Meldungen CLASSMARK ENQUIRY und CLASSMARK CHANGE

In Bild 23 folgt der Meldung PAGING RESPONSE die Meldung CLASSMARK CHANGE. (Tafel 23) und kurz darauf die Meldungen ClASSMARK ENQUIRY (Tafel 22). Letztere stellt eine Anfrage vom Netz an das Mobile dar („Nennen Sie Ihre Hard- und Software Parameter“), erstere die Antwort des Mobiles.

```
_____[ 436 ]___[ 1261500 ]___[ DOWN ]___[ RR ]_____________

06 13

06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages
13  00010011  MESSAGE TYPE        : CLASSMARK ENQUIRY
```

Tafel 21: Inhalt einer Meldung CLASSMARK ENQUIRY

CLASSMARK CHANGE enthält noch ein IE *Classmark 3*. Dieses IE ist vom Typ C (Conditional, nicht immer vorhanden) und vom Format TLV. Es enthält zahlreiche Informationen die dem jeweiligen Stand der Technik angepasst werden. Der interessierte Leser kann das verfolgen wenn er die Ausgabestände der Recommendation *ts_124008...* verfolgt.
Die Powerclass for GSM 1800 = 1 repräsentiert eine Leistung von 1 Watt und die Powerclass für P-GSM, E-GSM or R-GSM, = 4 eine Leistung von 2 Watt.
Interessant sind auch die Angaben zu den Umschaltzeiten des Mobiles (SM) um von einem Kanal zu einem anderen zu schalten, die 9/4 timeslots beträgt. Einschließlich Rücksprung (SMS) beträgt diese Zeit 14/4 timeslots.

```
_____[ 434 ]___[ 1261500 ]___[ UP ]___[ RR ]_____________

06 16 03 53  19 81 20 08  60 14 54 76  15 7b 00 00

06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages

16  00010110  MESSAGE TYPE        : CLASSMARK CHANGE

: Mobile Station Classmark 2
03  00000011  length              : 3

53  0-------  1 spare             : 0
    ---1----  "Controlled Early Classmark Sending" option is implemented in the MS
    ----0---  Encryp.Algor. A5_1  : available
    -----011  RF power capability : Class 4, handheld

19  0-------  1 spare bit         : 0
    -0------  pseudo-synch.capab. : not present
    --01----  SS Screening Indic. : phase 2 error handling
    ----1---  Mobile station supports mobile terminated point to point SMS
    -----0--  no VoiceBroadcastService (VBS) capability or no notifications wanted
    ------0-  no VoiceGroupCallService (VGCS) capability or no notifications wanted
    -------1  The MS does support the E-GSM or R-GSM

81  1-------  The MS does support any options that are indicated in CM3
    -0------  1 spare bit         : 0
    --0-----  LocationServiceValueAdded Capability  not supported
    ---0----  1 spare bit         : 0
    ----0---  SoLSA Capability    : not supported
    -----0--  Network initiated MO CM connection request not supported.
    ------0-  encryp.algorith.A5/3: not available
    -------1  encryp.algorith.A5/2: available


20  00100000  INFORMATION ELEMENT : CLASSMARK 3

08  00001000  length              : 8
          0   spare bit
        110   Multiband supported
: A5 bits
       0---   A5/7 not available
       -0--   A5/6 not available
```

```
        --0-  A5/5 not available
        ---0  A5/4 not available
: Associated Radio Capability 2
        0001  Powerclass for GSM 1800 = 1
: Associated Radio Capability 1
        0100  Powerclass for P-GSM, E-GSM or R-GSM, = 4
: R Support
           0  R Support not available
: HSCSD Multi Slot Capability
           1  HSCSD Multi Slot Capability
       01010  HSCSD Multi Slot Class = 10
: UniCodeSet2 treatment
           0  the ME has a preference for the default alphabet over UCS2.
: Extended Measurement Capability
           0  the MS does not support Extended Measurements
: Switch measurement capability
           1  MS measurement capability present
: SMS Value to succesive switch from one radio channel to another radio channel.
        1101  (13+1)/4 timeslots
: SM value to switch from one radio channel to another radio channel.
        1000  (8+1)/4 timeslots
: MS Positioning Method Capability
           0  MS Positioning Method Capability not present
: ECSD Multi Slot Capability
           1  ECSD Multi Slot Class
       01010  ECSD Multi Slot Class = 10
: 8-PSK Struct
           1  8-PSK Struct present
           1  8-PSK supported for uplink transmission and downlink reception
           1  8-PSK RF Power Capab.1 for 8-PSK modul. in GSM 400, GSM 700, GSM 850 or GSM 900.
          10  Power class E2
           1  8-PSK RF Power Capability 2 for 8-PSK modulation in GSM 1800 or GSM 1900
          10  Power class E2
: GSM 400 Bands Supported
           0  GSM 400 Bands Supported  not available
: GSM 850 Associated Radio Capability
           0  GSM 850 Associated Radio Capability  not available
           0  GSM 850 Associated Radio Capability  not available
: GSM 1900 Associated Radio Capability
           0  GSM 1900 Associated Radio Capability  not available
: UMTS FDD Radio Access Technology Capability
           0  UMTS FDD not supported
: UMTS 3.84 Mcps TDD Radio Access Technology Capability (1 bit field)
           0  UMTS 3.84 Mcps TDD not supported
: CDMA 2000 Radio Access Technology Capability (1 bit field)
           0  CDMA2000 not supported
: UMTS 3.84 Mcps TDD Radio Access Technology Capability
           0  UMTS FDD not supported
: CDMA 2000 Radio Access Technology Capability : bit >
           0  CDMA2000 not supported
: DTM GPRS Multi Slot Class
           0  DTM GPRS Multi Slot Class not available
: Single Slot DTM
           0  Single Slot DTM not supported
: DTM EGPRS Multi Slot Class
            0  DTM EGPRS Multi Slot Class not available
```

Tafel 22: Die Meldung CLASSMARK CHANGE

7.12 Die Meldung MEASUREMENT REPORT

Folgen wir dem Bild 23 so tritt jetzt die Meldung MEASUREMENT REPORT (Tafel 23) auf. Wie bereits bei der Besprechung des Aufbaus des TCH/F auf Tafel 14 erklärt wurde, misst dass Mobile regelmäßig (mindestens einmal in der Sekunde) sowohl den Empfangspegel der momentan in Anspruch genommenen Zelle, als auch die Empfangspegel der Nachbarzellen deren Frequenzen ihm in der SYSTEM INFORMATION TYPE 2 vom Netz übermittel wurden. Diese Messergebnisse werden im MEASUREMENT REPORT an das Netz übergeben.

Das Netz kann anhand der sich ändernden Empfangsbedingungen feststellen wann sich die MS der Zellgrenze nähert und kann dann bestimmen wenn ein *Hand Over* in eine andere Zelle erforderlich ist.

```
_____[ 413 ]___[ 1261762 ]___[ UP ]___[ RR ]_____________

06 15 99 19  01 a3 3b 48  09 e3 c2 e9  60 70 52 38  39 5b

06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages

15  00010101  MESSAGE TYPE        : MEASUREMENT REPORT

99  1-------  BA used             : yes
    -0------  Discontinous Transmission was not used
    --011001  RXLEV-FULL-SERVING-CELL= (-110 + 25) dB

19  0-------  spare               : 0
    -0------  MEAS-VALID          : yes
    --011001  RXLEV-SUB-SERVING-CELL = (-110 + 25) dB
     0------  spare               : 0
     -000---  RX-QUAL-FULL-SERVING-CELL = ~0,14% error bit
     ----000  RX-QUAL-SUB -SERVING-CELL = ~0,14% error bit
         110  Number of neighbouring cell measurements  = 6

      100011  RXLEV-Neighbour-CELL 1 = (-110 + 35) dB
       00111  BCCH-FREQ-NCELL 1   : 7
         011  NCC of the 1'th neighbouring cell = 3
         010  BCC of the 1'th neighbouring cell = 2

      010000  RXLEV-Neighbour-CELL 2 = (-110 + 16) dB
       00010  BCCH-FREQ-NCELL 2   : 2
         011  NCC of the second neighbouring cell = 3
         110  BCC of the second neighbouring cell = 6

      001111  RXLEV-Neighbour-CELL 3 = (-110 + 15) dB
       00001  BCCH-FREQ-NCELL 3   : 1
         011  NCC of the third neighbouring cell = 3
         101  BCC of the third neighbouring cell = 5

      001011  RXLEV-Neighbour-CELL 4 = (-110 + 11) dB
       00000  BCCH-FREQ-NCELL 4   : 0
         011  NCC of the fourth neighbouring cell = 3
         100  BCC of the fourth neighbouring cell = 4

      000101  RXLEV-Neighbour-CELL 5 = (-110 + 5) dB
       00100  BCCH-FREQ-NCELL 5   : 4
         011  NCC of the fifth neighbouring cell = 3
         100  BCC of the fifth neighbouring cell = 4

      000111  RXLEV-Neighbour-CELL 6 = (-110 + 7) dB
       00101  BCCH-FREQ-NCELL 6   : 5
         011  NCC of the sixth neighbouring cell = 3
         011  BCC of the sixth neighbouring cell = 3
```

Tafel 23: Inhalt einer Meldung MEASUREMENT REPORT

Der Inhalt der Meldung MEASUREMENT REPORT ist im hohem Maße selbstbeschreibend.
Z.B. wird mit RX-QUAL-FULL_SERVING-CELL auch die Fehlerrate auf der Arbeitsfrequenz gemeldet.
Diese Fehlerrate wird, da das Bitmuster der Trainingssequenz bekannt ist, aus dem Verhältnis der fehlerhaft übermittelten Bits zur Gesamtzahl der übertragen Bits in den Trainingssequenzen berechnet.

Zu erklären wäre noch der Begriff der SUB-SERVING-CELL. Im Zusammenhang mit der SYSTEM INFORMATION TYPE 3 war die Diskontinuierliche Sendung DTX genannt worden. Wenn diese aktiv ist, wird nicht jeder TDMA-Frame in die Messung einbezogen sondern nur die bei DTX gebrauchte Untermenge. Die in diesem Zusammenhang gemessene Felsstärke und Fehlerrate wird der SUB-SERVING-CELL zugeordnet.

7.13 Die Meldung CIPHERING MODE COMMAND

Die nächste RR-Meldung in der Übersicht Bild 23 wäre CIPHERING MODE COMMAND.
Diese Meldung ist offenbar sehr einfach. Das Netz weist an, den Algorithmus A5/1 zu verwenden und die IMEISV nicht mitzusenden.

```
_____[ 417 ]___[ 1261704 ]___[ DOWN ]___[ RR ]_____________

06 35 01

06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages

35  00110101  MESSAGE TYPE        : CIPHERING MODE COMMAND

01  ----000-  cipher with algorithm A5/1
    -------1  Start ciphering
    000-----  spare                : 0
    ---0----  Cipher Response      : IMEISV shall not be included
```

Tafel 24: Inhalt einer Meldung CIPHERING MODE COMMAND

Der Aufbau einer IMEI (International Mobile Station Equipment Identity) ist wie folgt:

- 3 Oktett TAC (*Type Approval Code*) Nachweise der bestandenen Prüfung des Geräts
- 1 Oktett FAC (*Final Assembly Code*) Hersteller
- 3 Oktett Seriennummer
- 4 Bit Reserve

Die IMEISV ist gleich der IMEI, aber anstelle der 4 Bit Reserve stehen 1 Oktett Software Versions-Nummer (SVR).

7.14 Die Meldung CIPHERING MODE COMPLETE

Die Meldung CIPHERING MODE COMPLETE (Tafel 25) ist demnach sehr einfach aufgebaut.

```
_____[ 415 ]___[ 1261704 ]___[ UP ]___[ RR ]_____________

06 32

06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages
32  00110010  MESSAGE TYPE        : CIPHERING MODE COMPLETE
```

Tafel 25: Inhalt einer Meldung CIPHERING MODE COMPLETE

7.15 Die Meldung ASSIGNMENT COMMAND

Bei der Besprechung der RR-Messages sind wir bisher weitestgehend nach deren Auftreten in Bild 23 vorgegangen. In dem gelb hinterlegten Bereich, in dem das Mobile mit dem Netz über die Parameter der durchzuschaltenden Verbindung verhandelt, waren bereits die im Abschnitt 8 zu behandelnden Mobility Management Messages AUTHENTIFICATION REQUEST, AUTHENTIFICATION RESPONSE, IDENTITY REQUEST und IDENTITY RESPONSE aufgetreten.
Nunmehr hat die Gegenseite (der ISDN-Partner) noch die Meldung SETUP geschickt, die vom Mobile mit CALL CONFIRMED bestätigt wird.
Das Netz muss nunmehr einen Transportkanal zuweisen, was mit der Meldung ASSIGNMENT COMMAND erfolgt

.

```
_____[ 384 ]___[ 1262112 ]___[ DOWN ]___[ RR ]_____________
```

```
06 2e 0f 40  55 05 63 41  03 02 28 80

06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages

2e  00101110  MESSAGE TYPE        : ASSIGNMENT COMMAND

: Channel Description 2
0f  00001---  Channel type and TDMA offset = TCH/F + ACCHs
    -----111  Timslot number      : 7

40  010-----  Training sequ. code : 2
    ---000--  Single channel      : RF single channel
    ------00  Sgl RF chan.high prt: 0
55  01010101  abs.RFchan. low part: 85

: POWER LEVEL
05  000-----  spare
    ---00101  Power level         : 5

: Channel Mode

63  01100011  INFORMATION ELEMENT : CHANNEL MODE
41  01000001  channel mode        : speech full rate or half rate version 3
```

Tafel 26. Die Meldung ASSIGNMENT COMMAND

In der Meldung ASSIGNMENT COMMAND auf Tafel 26 :

- wird ein TCH/F zugewiesen in dessen TDMA Rahmen ein ACCH eingebettet ist, wie mit Bild 14 erklärt wurde
- Die Nummer des Zeitschlitzes ist 7
- Es handelt sich um einen einzelnen Kanal der Nummer 85 mit dem TrainingsSequence Code 2
- Der Power level 5 (0,8 W) wird vorgeschrieben

Es sei in diesem Zusammenhang noch etwas zu *full rate* und *half rate* Kanälen gesagt:
Wie bei der Beschreibung der TRAU erläutert, wird der PCM-Kanal mit seiner 64 kbit Sprachübertragung zu nächst geviertelt. Die 4 Unterkanäle werden durch einen hochkomplexen Algorithmus zu einer Datenrate von 13 kbit/sec komprimiert. Wie aus der Erfahrung bekannt ist die dabei erreichte Sprachqualität ausgezeichnet. Aus Gründen der Frequenzökonomie wurde beschlossen für spezielle Fälle den 64 kbit Kanal in 8 Sprachkanäle zu unterteilen wobei die effektive Sprachdatenrate 6.5 kbit/sec beträgt. Dieser Kanal mit der halben Datenrate (half rate) wurde vom Autor bei seinen Mobile-Verbindungen noch nicht angetroffen, weshalb noch keine Erfahrungen über die Sprachqualität vorliegen.

7.16 Die Meldung ASSIGNMENT COMPLETE

Die Meldung ASSIGNMENT COMPLETE ist sehr einfach, als Grund für die Meldung ist hier *Normal event* eingetragen, das normale Ereignis.

```
_____[ 24 ]___[ 12:02:44,492 ]___[ UP ]_____________________________________________

06 29 00

06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages

29  00101001  MESSAGE TYPE        : ASSIGNMENT COMPLETE

00  00000000  RR-Cause (reason of event) = Normal event
```

Tafel 27: Inhalt einer Meldung ASSIGNMENT COMPLETE

In Tafel 28 ist ein Teil des Scriptes für ASSIGNMENT COMPLETE angegeben , da sind alle möglichen Ereignisse aufgeführt.

```
00000000  RR-Cause (reason of event) = Normal event
00000001  RR-Cause (reason of event) = Abnormal release, unspecified
00000010  RR-Cause (reason of event) = Abnormal release, channel unacceptable
00000011  RR-Cause (reason of event) = Abnormal release, timer expired
00000100  RR-Cause (reason of event) = Abnormal release, no activity on the radio path
00000101  RR-Cause (reason of event) = Preemptive release
00001000  RR-Cause (reason of event) = Handover impossible, timing advance out of range
00001001  RR-Cause (reason of event) = Channel mode unacceptable
00001010  RR-Cause (reason of event) = Frequency not implemented
01000001  RR-Cause (reason of event) = Call already cleared
01011111  RR-Cause (reason of event) = Semantically incorrect message
01100000  RR-Cause (reason of event) = Invalid mandatory information
01100001  RR-Cause (reason of event) = Message type non-existent or not implemented
01100010  RR-Cause (reason of event) = Message type not compatible with protocol state
01100100  RR-Cause (reason of event) = Conditional IE error
01100101  RR-Cause (reason of event) = Nocell allocation available
01101111  RR-Cause (reason of event) = Protocol error unspecified
```

Tafel 28: Gründe die in der Meldung ASSIGNMENT COMPLETE vorkommen können

7.17 Die Meldung CHANNEL RELEASE

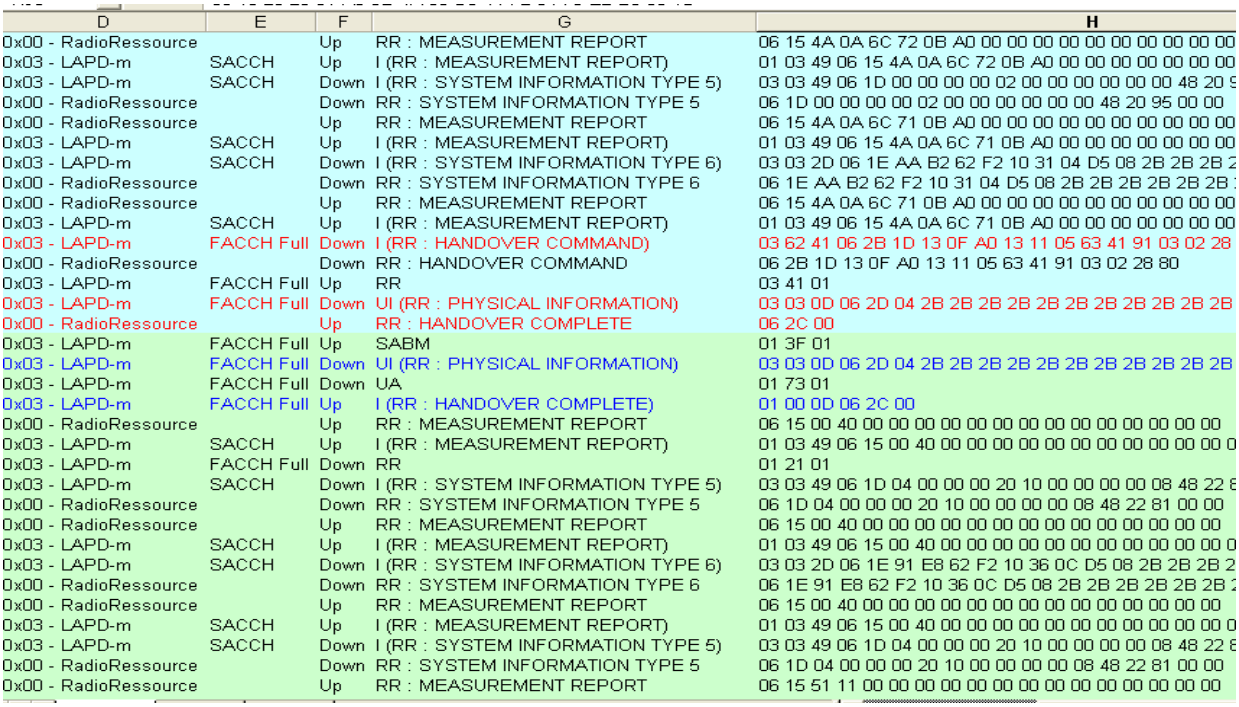
Mit der Meldung CHANNEL RELEASE (Tafel 29) wird der Transportkanal wieder abgegeben. Als RR-cause sind wieder die in Tafel 28 aufgeführten Gründe möglich.

```
____[ 79 ]___[ 14:12:23,910 ]___[ DOWN ]____[ FACCH_F ]_____________________________

06 0d 00

06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages

0d  00001101  MESSAGE TYPE        : CHANNEL RELEASE

00  00000000  RR-Cause (reason of event) = Normal event
```

Tafel 29: Inhalt einer Meldung CHANNEL RELEASE

7.18 Die Prozedur HANDOVER

In Bild 34 ist eine Handoverprozedur dargestellt. Sie können den Traceausschnitt als eine Fortsetzung des in Bild 23 dargestellten Traces auffassen. Mit dem Mobile wird während der Verbindung (des Gesprächs) ein Ortswechsel vorgenommen. Aus den MEASUREMENT REPORTS erkennt der BSC dass sich das Mobile bei immer kleiner werdenden C1-Werten der aktuellen Zelle auf eine Zelle zubewegt deren Feldstärke (und die C1-Werte) immer größer werden. Schließlich weist das Netz mit dem in Tafel 30 dargestellten Kommando das Handover an. Mit der in Tafel 31 dargestellten Meldung PHYSICAL INFORMATION wird dem Mobile der neue Timing advance Wert zugewiesen. Das Mobile fordert mit SABME erneut den *acknowledge Mode* an. Damit beginnt im grün hinterlegten Bereich auf Bild 34 das Zählen der Meldungen erneut bei Null. Die Meldung HANDOVER COMPLETE wird im neuen *acknowledged mode* zum Netz geschickt.



D	E	F	G	H
0x00 - RadioRessource		Up	RR : MEASUREMENT REPORT	06 15 4A 0A 6C 72 0B A0 00 00 00 00 00 00 00 00 00
0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 4A 0A 6C 72 0B A0 00 00 00 00 00 00 00
0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 5)	03 03 49 06 1D 00 00 00 00 02 00 00 00 00 00 00 48 20 9
0x00 - RadioRessource		Down	RR : SYSTEM INFORMATION TYPE 5	06 1D 00 00 00 00 02 00 00 00 00 00 00 48 20 95 00 00
0x00 - RadioRessource		Up	RR : MEASUREMENT REPORT	06 15 4A 0A 6C 71 0B A0 00 00 00 00 00 00 00 00 00
0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 4A 0A 6C 71 0B A0 00 00 00 00 00 00 00
0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 6)	03 03 2D 06 1E AA B2 62 F2 10 31 04 D5 08 2B 2B 2B 2
0x00 - RadioRessource		Down	RR : SYSTEM INFORMATION TYPE 6	06 1E AA B2 62 F2 10 31 04 D5 08 2B 2B 2B 2B 2B 2B 1
0x00 - RadioRessource		Up	RR : MEASUREMENT REPORT	06 15 4A 0A 6C 71 0B A0 00 00 00 00 00 00 00 00 00
0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 4A 0A 6C 71 0B A0 00 00 00 00 00 00 00
0x03 - LAPD-m	FACCH Full	Down	I (RR : HANDOVER COMMAND)	03 62 41 06 2B 1D 13 0F A0 13 11 05 63 41 91 03 02 28
0x00 - RadioRessource		Down	RR : HANDOVER COMMAND	06 2B 1D 13 0F A0 13 11 05 63 41 91 03 02 28 80
0x03 - LAPD-m	FACCH Full	Up	RR	03 41 01
0x03 - LAPD-m	FACCH Full	Down	UI (RR : PHYSICAL INFORMATION)	03 03 0D 06 2D 04 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B
0x00 - RadioRessource		Up	RR : HANDOVER COMPLETE	06 2C 00
0x03 - LAPD-m	FACCH Full	Up	SABM	01 3F 01
0x03 - LAPD-m	FACCH Full	Down	UI (RR : PHYSICAL INFORMATION)	03 03 0D 06 2D 04 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B
0x03 - LAPD-m	FACCH Full	Down	UA	01 73 01
0x03 - LAPD-m	FACCH Full	Up	I (RR : HANDOVER COMPLETE)	01 00 0D 06 2C 00
0x00 - RadioRessource		Up	RR : MEASUREMENT REPORT	06 15 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00
0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 00 40 00 00 00 00 00 00 00 00 00 00 0
0x03 - LAPD-m	FACCH Full	Down	RR	01 21 01
0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 5)	03 03 49 06 1D 04 00 00 00 20 10 00 00 00 00 08 48 22 8
0x00 - RadioRessource		Down	RR : SYSTEM INFORMATION TYPE 5	06 1D 04 00 00 00 20 10 00 00 00 00 08 48 22 81 00 00
0x00 - RadioRessource		Up	RR : MEASUREMENT REPORT	06 15 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00
0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 00 40 00 00 00 00 00 00 00 00 00 00 0
0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 6)	03 03 2D 06 1E 91 E8 62 F2 10 36 0C D5 08 2B 2B 2B 2
0x00 - RadioRessource		Down	RR : SYSTEM INFORMATION TYPE 6	06 1E 91 E8 62 F2 10 36 0C D5 08 2B 2B 2B 2B 2B 2B 2
0x00 - RadioRessource		Up	RR : MEASUREMENT REPORT	06 15 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00
0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 00 40 00 00 00 00 00 00 00 00 00 00 0
0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 5)	03 03 49 06 1D 04 00 00 00 20 10 00 00 00 00 08 48 22 8
0x00 - RadioRessource		Down	RR : SYSTEM INFORMATION TYPE 5	06 1D 04 00 00 00 20 10 00 00 00 00 08 48 22 81 00 00
0x00 - RadioRessource		Up	RR : MEASUREMENT REPORT	06 15 51 11 00 00 00 00 00 00 00 00 00 00 00 00 00

Bild 34: Traceausschnitt mit Handover messages

Beim Handover unterscheidet man:

- den Intra-BSC-Handover, bei dem die MS die BTS wechselt, aber im Bereich eines BSC bleibt,
- den Intra-MSC-Handover, hier wechselt die MS das BSC verbleibt aber im gleichen MSC,
- den Inter-MSC-Handover, bei dem sogar der MSC Bereich gewechselt wird.

Es ist auch ein Frequenzwechsel innerhalb einer BTS denkbar, dieser wird aber normalerweise mit einer ASSIGNMENT COMMAND Meldung bewerkstelligt.

Die in Bild 34 dargestellte Handover-Procedur ist nicht wirklich durch einen Ortswechsel zustande gekommen. SAGEM Trace-Mobiles besitzen eine sog. *Forcing Function,* mit der man z.B. Handover erzwingen kann. Im Fenster von OT Drive 4 wurde dazu die Funktion *Forcing* aufgerufen und im sich öffnenden Menü *Cell Forcing* für den BCCH 19 aktiviert.

OT Drive 4 hat daraufhin die Meldung MEASUREMENT REPORT manipuliert. Dem BSC wurde vorgetäuscht , dass die Feldstärke der benachbarten BTS mit dem BCCH = 19 plötzlich viel stärker ist als die der aktuellen Zelle. Aus dem MEASUREMENT REPORT in Tafel 23 entnimmt man, dass die Zelle mit dem NCC 3 und BCC 5 ursprünglisch nur eine Feldstärke von –95 dB besitzt. Durch Manipulation ist ihre scheinbare Feldstärke auf –61 dB erhöht worden, was zum Auslösen des Hanover führte.
Das BSC gab daraufhin den Befehl zum Handover. Das Ergebnis ist in Bild 34 dargestellt

```
_____[ 369 ]___[ 92380 ]___[ DOWN ]___[ RR ]_____________

06 2b 1d 13  0f a0 13 11  05 63 41 91  03 02 28 80

06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages
2b  00101011  MESSAGE TYPE        : HANDOVER COMMAND

: Celldescription
```

```
1d  --011---  PLMN Colour Code NCC: 3
    -----101  BS Colour code  BCC : 5
    00------  BCCH ARFCN high part: 0
13  00010011  BCCH ARFCN low part : 19

: Channel Description 2
0f  00001---  Channel type and TDMA offset = TCH/F + ACCHs
    -----111  Timslot number      : 7

a0  101-----  Training sequ. code : 5
    ---000--  Single channel      : RF single channel
    ------00  Sgl RF chan.high prt: 0
13  00010011  abs.RFchan. low part: 19

: Handover Reference
11  00010001  Handover refer. val.: 17

: Power Command and Access Type
05  0-------  Sending of Handover access is mandatory
    -00-----  spare
    ---00101  Power Level         : 5
```

Tafel 30: Inhalt einer Meldung HANDOVER COMMAND

In der Meldung HANDOVER COMMAND (Tafel 31) sieht man die Beschreibung der neuen Zelle (BCCH = 19) in die gewechselt werden soll und in PHYSICAL INFORMATION (Tafel 32) wird der neue Timing Advance Wert übergeben. Die *Handover Reference* ist eine Zufallszahl mit der das Kommando gekennzeichnet wird.

```
_____[ 367 ]___[ 92401 ]___[ DOWN ]___[ LAPDm ]_____________

03 03 0d 06  2d 04 2b 2b  2b 2b 2b 2b  2b 2b 2b 2b  2b 2b 2b 2b
2b 2b 2b

03  0-------  Spare               : 0
    -00-----  Link Prot. Disc.    : 1
    ---000--  SAPI                : 0
    ------1-  C/R Flag            : 1, BS side to MS side
    -------1  EA                  : 1
03  00000011  Unnumbered          : UNNUMBERED INFORMATION    P=0
0d  000011--  length              : 3
    ------0-  M                   : 0
    -------1  EL                  : 1
06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages
2d  00101101  MESSAGE TYPE        : PHYSICAL INFORMATION
: Timing Advance
04  00------  spare
    --000100  Timing advance value: 4 x 48/13 sec
```

Tafel 31: Inhalt einer Meldung PHYSICAL INFORMATION

Der konkrete Wert der sich hinter dem Powerlevel 5 in der Meldung HANDOVER COMMAND verbirgt ist nachstehender Übersicht aus der Recommendation GSM 05.05 zu entnehmen.

Power control level:	0-2	3	4	**5** …	16	17	18	19-31
Nominal Output power(dBm):	39	37	35	**33** …	11	9	7	5

Man erkennt, dass eine Differenz von einem Punkt im *Power control level* eine Differenz von 2dBm darstellt.

.

```
_____[ 366 ]___[ 92401 ]___[ UP ]___[ RR ]_____________

06 2c 00
```

```
06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages
2c  00101100  MESSAGE TYPE        : HANDOVER COMPLETE

: RR Cause
00  00000000  Normal event
```

Tafel 32: Inhalt einer Meldung HANDOVER COMPLETE

8. Die Meldungen für das Mobility Management

Bild 35 zeigt den Beginn eines MOC-Traces, der im sichtbaren Teil die Meldungen CM SERVICE REQUEST, AUTHENTIFICATION REQUEST und AUTHENTIFICATIOn RESPONS enthält.

D	E	F	G	H
0x00 - RadioRessource		Down	RR : PAGING REQUEST TYPE 1	06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B 2B 2B 2
0x03 - LAPD-m	RACH	Up	RR CHANNEL REQUEST	FD
0x03 - LAPD-m	CCCH	Down	(RR : PAGING REQUEST TYPE 1)	15 06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B 2B 2
0x00 - RadioRessource		Down	RR : PAGING REQUEST TYPE 1	06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B 2B 2B 2
0x03 - LAPD-m	CCCH	Down	(RR : PAGING REQUEST TYPE 1)	15 06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B 2B 2
0x00 - RadioRessource		Down	RR : PAGING REQUEST TYPE 1	06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B 2B 2B 2
0x03 - LAPD-m	BCCH	Down	(RR : SYSTEM INFORMATION TYPE 4)	31 06 1C 62 F2 10 31 04 65 04 A5 00 00 11 2B 2B
0x00 - RadioRessource		Down	RR : SYSTEM INFORMATION TYPE 4	06 1C 62 F2 10 31 04 65 04 A5 00 00 11 2B 2B 2B
0x03 - LAPD-m	CCCH	Down	(RR : IMMEDIATE ASSIGNMENT)	2D 06 3F 03 41 40 55 FD 05 0C 02 00 2B 2B 2B 2E
0x00 - RadioRessource		Down	RR : IMMEDIATE ASSIGNMENT	06 3F 03 41 40 55 FD 05 0C 02 00 2B 2B 2B 2E
0x02 - NAS		Up	MM : CM SERVICE REQUEST	05 24 11 03 53 19 81 05 F4 87 54 62 CD
0x03 - LAPD-m	SDCCH	Up	SABM (MM : CM SERVICE REQUEST)	01 3F 35 05 24 11 03 53 19 81 05 F4 87 54 62 CD
0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 6)	03 03 2D 06 1E AA B2 62 F2 10 31 04 55 08 2B 2E
0x00 - RadioRessource		Down	RR : SYSTEM INFORMATION TYPE 6	06 1E AA B2 62 F2 10 31 04 55 08 2B 2B 2B 2B 2I
0x03 - LAPD-m	SDCCH	Down	UA (MM : CM SERVICE REQUEST)	01 73 35 05 24 11 03 53 19 81 05 F4 87 54 62 CD
0x00 - RadioRessource		Up	RR : CLASSMARK_CHANGE	06 16 03 53 19 81 20 08 60 14 54 76 15 7B 00 00
0x03 - LAPD-m	SDCCH	Up	I (RR : CLASSMARK_CHANGE)	01 00 41 06 16 03 53 19 81 20 08 60 14 54 76 15 7
0x03 - LAPD-m	SDCCH	Down	I (RR : CLASSMARK ENQUIRY)	03 20 09 06 13 2B 2B 2B 2B 2B 2B 2B 2B 2B 2
0x00 - RadioRessource		Down	RR : CLASSMARK ENQUIRY	06 13
0x00 - RadioRessource		Up	RR : CLASSMARK_CHANGE	06 16 03 53 19 81 20 08 60 14 54 76 15 7B 00 00
0x00 - RadioRessource		Up	RR : MEASUREMENT REPORT	06 15 A5 25 01 A5 3B 4F A1 A2 42 EA C2 78 50 3A
0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 A5 25 01 A5 3B 4F A1 A2 42 EA C2
0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 5)	03 03 49 06 1D 00 00 00 00 02 00 00 00 00 00 00 4
0x00 - RadioRessource		Down	RR : SYSTEM INFORMATION TYPE 5	06 1D 00 00 00 00 02 00 00 00 00 00 00 48 20 95 0
0x03 - LAPD-m	SDCCH	Down	I (MM : AUTHENTIFICATION REQUEST)	03 42 4D 05 12 01 5E 44 C3 C3 EB B2 87 D5 CE 4
0x02 - NAS		Down	MM : AUTHENTIFICATION REQUEST	05 12 01 5E 44 C3 C3 EB B2 87 D5 CE 4C 88 4F 7
0x03 - LAPD-m	SDCCH	Up	I (RR : CLASSMARK_CHANGE)	01 44 41 06 16 03 53 19 81 20 08 60 14 54 76 15 7
0x02 - NAS		Up	MM : AUTHENTIFICATION RESPONSE	05 54 77 45 35 A6
0x03 - LAPD-m	SDCCH	Down	RR	01 61 01
0x03 - LAPD-m	SDCCH	Up	I (MM : AUTHENTIFICATION RESPONSE)	01 46 19 05 54 77 45 35 A6
0x00 - RadioRessource		Up	RR : MEASUREMENT REPORT	06 15 00 40 00 00 00 00 00 00 00 00 00 00 00 0
0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 00 40 00 00 00 00 00 00 00 00 0
0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 6)	03 03 2D 06 1E AA B2 62 F2 10 31 04 D5 08 2B 2E

Bild 35: Auszug aus dem Trace eines Mobile Originated Call (MOC)

Das Mobility Management umfasst folgende Gebiete:

- Die Registration des Mobiles im Netz (Registration messages)
- Das Sicherheitsmanagement (Security messages)
- Das Verbindungs- Management (**C**onnection **M**anagement messages)
- Verschiedenes (Miscellaneous messages)

Beim Mobile Terminated Call waren zwei Mobilty Management Messages aufgetreten. Es waren die Meldungen AUTHENTICATION REQUEST auf Tafel 19 und AUTHENTICATION RESPONSE. Auf Tafel 20. Sie zählen zum Sicherheitsmanagement (Security messages).

.

8.1 Die Meldung CM SERVICE REQUEST

Nach Eingabe der Telefonnummer in das Mobile, und Abheben des Hörers (durch Tastendruck), übergibt die Schicht 3 einen CM SERVICE REQUEST an die Schicht 2. Die Schicht 2 kann zu diesem Zeitpunkt diese Anforderung nicht weitergeben, sondern muss zunächst einen Kanal anfordern. Dieser Vorgang ist in Bild 30 rot eingezeichnet.
Das Netz schickt die bekannte Meldung IMMEDIATE ASSIGNMENT, mit der dem Mobile ein Arbeitskanal zugewiesen wird Die Meldung CM SERVICE REQUEST kann daraufhin kombiniert mit einem SABM (Anforderung des acknowledged mode) an das Netz gesandt werden
In der Meldung CM SERVICE REQUEST (Tafel 33) steht natürlich als erstes der „Requested service type“ der anzufordernde Dienst und dann die Informationselemente *Mobile Station Classmark 2* und *Mobile Identity* die wir aus der Meldung PAGING RESPONSE kennen.

```
_____[ 300 ]___[ 4533728 ]___[ UP ]___[ NAS ]_____________

05 24 11 03  53 19 81 05  f4 87 54 62  cd

05  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0101  Protocol Discrim.   : mobility management messages non GPRS
24  00------  SendSequenceNumber  : 0

    --100100  MESSAGE TYPE        : CM SERVICE REQUEST

11  0-------  spare               : 0
    -001----  value for the ciphering key sequence number = 1
    ----0001  Requ.service type   : Mobile originating call establishment, or p.m.conn.estab.

: Mobile Station Classmark 2
03  00000011  length              : 3
53  0-------  1 spare             : 0
    ---1----  "Controlled Early Classmark Sending" option is implemented in the MS
    ----0---  Encryp.Algor. A5_1  : available
    -----011  RF power capability : Class 4, handheld
19  0-------  1 spare bit         : 0
    -0------  pseudo-synch.capab. : not present
    --01----  SS Screening Indic. : phase 2 error handling
    ----1---  Mobile station supports mobile terminated point to point SMS
    -----0--  no VoiceBroadcastService (VBS) capability or no notifications wanted
    ------0-  no VoiceGroupCallService (VGCS) capability or no notifications wanted
    -------1  The MS does support the E-GSM or R-GSM
81  1-------  The MS does support any options that are indicated in CM3
    -0------  1 spare bit         : 0
    --0-----  LocationServiceValueAdded Capability  not supported
    ---0----  1 spare bit         : 0
    ----0---  SoLSA Capability    : not supported
    -----0--  Network initiated MO CM connection request not supported.
    ------0-  encryp.algorith.A5/3: not available
    -------1  encryp.algorith.A5/2: available

: Mobile identity
05  00000101  length              : 5
f4  ----0---  No. of ID digits    : even
    -----100  Type of identity    : TMSI/P-TMSI
    1111----  Identity Digit 1    : 95
87  10000111  Identity Digit 2,3  : take hex value
54  01010100  Identity Digit 4,5  : take hex value
62  01100010  Identity Digit 6,7  : take hex value
cd  11001101  Identity Digit 8,9  : take hex value
c4  11000100  Identity Digit 8,9  : take hex value
```

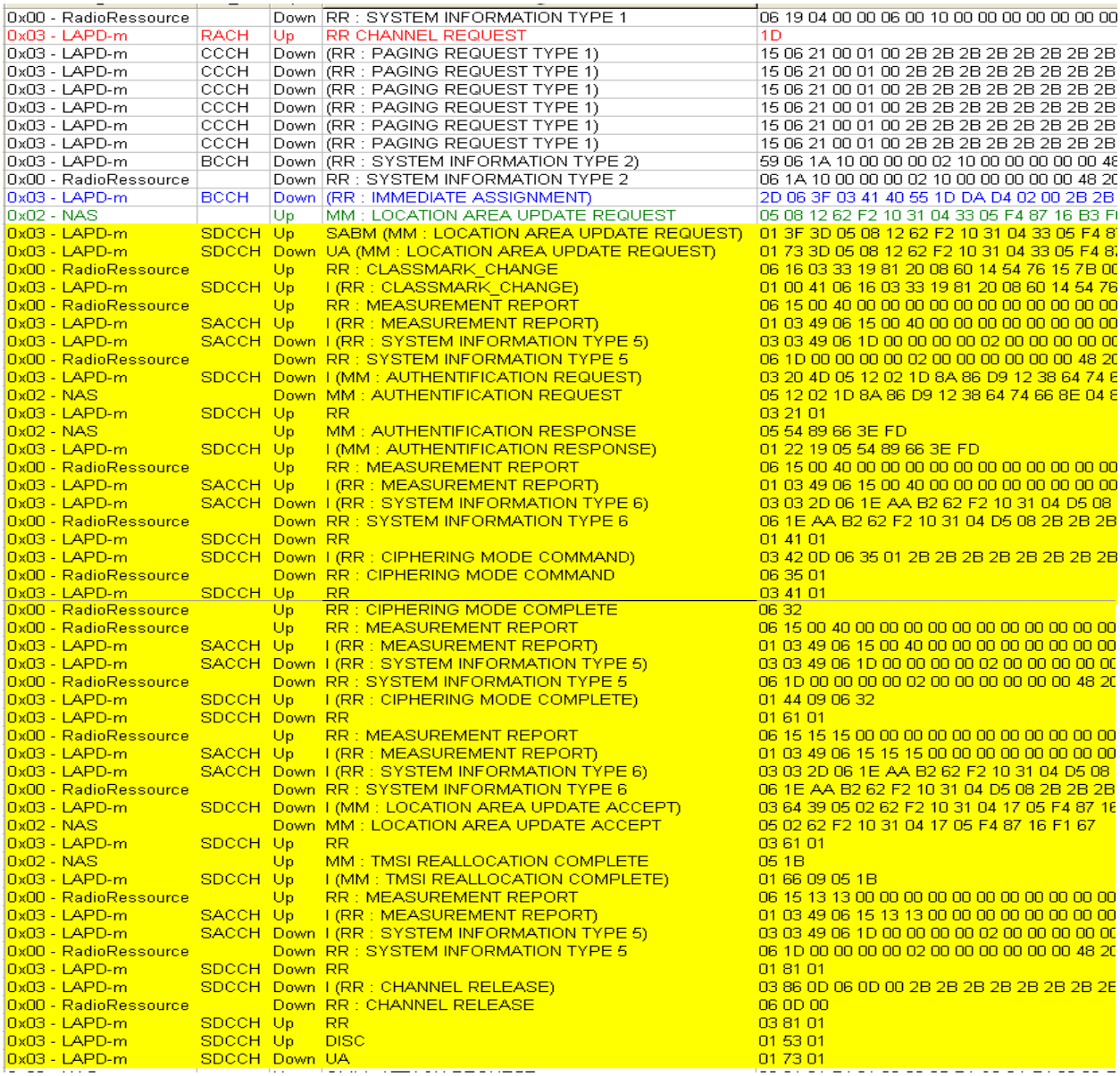
Tafel 33: Inhalt einer Meldung CM SERVICE REQUEST

Weitere **C**onnection **M**anagement Messages sind:
Die Variationen zu CM SERVICE REQUEST, d.h. die Meldungen CM SERVICE REJECT, CM SERVICE RESPONSE, CM SERVICE ACCEPT und CM SERVICE ABORT sowie CM RE-ESTABLISHMENT REQUEST und ABORT. Wir wolle darauf hier nicht näher eingehen.

Die meisten Meldungen für das *Mobility Management* sind in der Operation Location Update enthalten.

8.2 Das Location Update

Im Abschnitt 5.5.1 wurde beschrieben, wie das Mobile nach dem Einschalten den stärksten Sender mit dem *Network Color Code* seines Operators findet. Wenn das Mobile die zuständige Mobilfunkzelle gefunden hat muss es sich dort anmelden. Die dabei ausgetauschten Informationen sind im Bild 31 dargestellt.



0x00 - RadioRessource		Down	RR : SYSTEM INFORMATION TYPE 1	06 19 04 00 00 06 00 10 00 00 00 00 00 00 00
0x03 - LAPD-m	RACH	Up	RR CHANNEL REQUEST	1D
0x03 - LAPD-m	CCCH	Down	(RR : PAGING REQUEST TYPE 1)	15 06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B
0x03 - LAPD-m	CCCH	Down	(RR : PAGING REQUEST TYPE 1)	15 06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B
0x03 - LAPD-m	CCCH	Down	(RR : PAGING REQUEST TYPE 1)	15 06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B
0x03 - LAPD-m	CCCH	Down	(RR : PAGING REQUEST TYPE 1)	15 06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B
0x03 - LAPD-m	CCCH	Down	(RR : PAGING REQUEST TYPE 1)	15 06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B
0x03 - LAPD-m	CCCH	Down	(RR : PAGING REQUEST TYPE 1)	15 06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B
0x03 - LAPD-m	BCCH	Down	(RR : SYSTEM INFORMATION TYPE 2)	59 06 1A 10 00 00 00 02 10 00 00 00 00 46
0x00 - RadioRessource		Down	RR : SYSTEM INFORMATION TYPE 2	06 1A 10 00 00 00 02 10 00 00 00 00 48 20
0x03 - LAPD-m	BCCH	Down	(RR : IMMEDIATE ASSIGNMENT)	2D 06 3F 03 41 40 55 1D DA D4 02 00 2B 2B
0x02 - NAS		Up	MM : LOCATION AREA UPDATE REQUEST	05 08 12 62 F2 10 31 04 33 05 F4 87 16 B3 F
0x03 - LAPD-m	SDCCH	Up	SABM (MM : LOCATION AREA UPDATE REQUEST)	01 3F 3D 05 08 12 62 F2 10 31 04 33 05 F4 87
0x03 - LAPD-m	SDCCH	Down	UA (MM : LOCATION AREA UPDATE REQUEST)	01 73 3D 05 08 12 62 F2 10 31 04 33 05 F4 87
0x00 - RadioRessource		Up	RR : CLASSMARK_CHANGE	06 16 03 33 19 81 20 08 60 14 54 76 15 7B 00
0x03 - LAPD-m	SDCCH	Up	I (RR : CLASSMARK_CHANGE)	01 00 41 06 16 03 33 19 81 20 08 60 14 54 76
0x00 - RadioRessource		Up	RR : MEASUREMENT REPORT	06 15 00 40 00 00 00 00 00 00 00 00 00 00 00
0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 00 40 00 00 00 00 00 00 00 00
0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 5)	03 03 49 06 1D 00 00 00 00 02 00 00 00 00 00
0x00 - RadioRessource		Down	RR : SYSTEM INFORMATION TYPE 5	06 1D 00 00 00 00 02 00 00 00 00 00 48 20
0x03 - LAPD-m	SDCCH	Down	I (MM : AUTHENTIFICATION REQUEST)	03 20 4D 05 12 02 1D 8A 86 D9 12 38 64 74 6
0x02 - NAS		Down	MM : AUTHENTIFICATION REQUEST	05 12 02 1D 8A 86 D9 12 38 64 74 66 8E 04 6
0x03 - LAPD-m	SDCCH	Up	RR	03 21 01
0x02 - NAS		Up	MM : AUTHENTIFICATION RESPONSE	05 54 89 66 3E FD
0x03 - LAPD-m	SDCCH	Up	I (MM : AUTHENTIFICATION RESPONSE)	01 22 19 05 54 89 66 3E FD
0x00 - RadioRessource		Up	RR : MEASUREMENT REPORT	06 15 00 40 00 00 00 00 00 00 00 00 00 00 00
0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 00 40 00 00 00 00 00 00 00 00
0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 6)	03 03 2D 06 1E AA B2 62 F2 10 31 04 D5 08
0x00 - RadioRessource		Down	RR : SYSTEM INFORMATION TYPE 6	06 1E AA B2 62 F2 10 31 04 D5 08 2B 2B 2B
0x03 - LAPD-m	SDCCH	Down	RR	01 41 01
0x03 - LAPD-m	SDCCH	Down	I (RR : CIPHERING MODE COMMAND)	03 42 0D 06 35 01 2B 2B 2B 2B 2B 2B 2B 2B
0x00 - RadioRessource		Down	RR : CIPHERING MODE COMMAND	06 35 01
0x03 - LAPD-m	SDCCH	Up	RR	03 41 01
0x00 - RadioRessource		Up	RR : CIPHERING MODE COMPLETE	06 32
0x00 - RadioRessource		Up	RR : MEASUREMENT REPORT	06 15 00 40 00 00 00 00 00 00 00 00 00 00 00
0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 00 40 00 00 00 00 00 00 00 00
0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 5)	03 03 49 06 1D 00 00 00 00 02 00 00 00 00 00
0x00 - RadioRessource		Down	RR : SYSTEM INFORMATION TYPE 5	06 1D 00 00 00 00 02 00 00 00 00 00 48 20
0x03 - LAPD-m	SDCCH	Up	I (RR : CIPHERING MODE COMPLETE)	01 44 09 06 32
0x03 - LAPD-m	SDCCH	Down	RR	01 61 01
0x00 - RadioRessource		Up	RR : MEASUREMENT REPORT	06 15 15 15 00 00 00 00 00 00 00 00 00 00 00
0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 15 15 00 00 00 00 00 00 00 00
0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 6)	03 03 2D 06 1E AA B2 62 F2 10 31 04 D5 08
0x00 - RadioRessource		Down	RR : SYSTEM INFORMATION TYPE 6	06 1E AA B2 62 F2 10 31 04 D5 08 2B 2B 2B
0x03 - LAPD-m	SDCCH	Down	I (MM : LOCATION AREA UPDATE ACCEPT)	03 64 39 05 02 62 F2 10 31 04 17 05 F4 87 16
0x02 - NAS		Down	MM : LOCATION AREA UPDATE ACCEPT	05 02 62 F2 10 31 04 17 05 F4 87 16 F1 67
0x03 - LAPD-m	SDCCH	Up	RR	03 61 01
0x02 - NAS		Up	MM : TMSI REALLOCATION COMPLETE	05 1B
0x03 - LAPD-m	SDCCH	Up	I (MM : TMSI REALLOCATION COMPLETE)	01 66 09 05 1B
0x00 - RadioRessource		Up	RR : MEASUREMENT REPORT	06 15 13 13 00 00 00 00 00 00 00 00 00 00 00
0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 13 13 00 00 00 00 00 00 00 00
0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 5)	03 03 49 06 1D 00 00 00 00 02 00 00 00 00 00
0x00 - RadioRessource		Down	RR : SYSTEM INFORMATION TYPE 5	06 1D 00 00 00 00 02 00 00 00 00 00 48 20
0x03 - LAPD-m	SDCCH	Down	RR	01 81 01
0x03 - LAPD-m	SDCCH	Down	I (RR : CHANNEL RELEASE)	03 86 0D 06 0D 00 2B 2B 2B 2B 2B 2B 2B 2B
0x00 - RadioRessource		Down	RR : CHANNEL RELEASE	06 0D 00
0x03 - LAPD-m	SDCCH	Up	RR	03 81 01
0x03 - LAPD-m	SDCCH	Up	DISC	01 53 01
0x03 - LAPD-m	SDCCH	Down	UA	01 73 01

Bild 36: Trace eines Location Update

In Bild 31 ist wieder der typische Übergang vom idle Mode zum dedicated Mode zu sehen. Auf der Schicht 2 wird eine Kanal angefordert (Tafel 34), das Netz reagiert mit Zuweisung des Kanals durch die Meldung IMMEDIATE ASSIGNMENT.

```
_____[ 237 ]___[ 18884 ]___[ UP ]___[ LAPDm ]_____________

1d

L2-RACH Channel Request
```

```
1d  0001----  Location updating and the network does not set NECI bit to 1
```

Tafel 34: Inhalt einer Meldung CHANNEL REQUEST beim Location Update

In Tafel 34 bedeuted NECI den *New Establishment Cause Indicator*, der hier nicht gleich „1“ gesetzt wird. Das bedeutet, dass es sich nicht um eine neue Verbindung handelt wie z.B. auch bei einem Handover, bei dem in einer bestehenden Verbindung die Zelle gewechselt wird.

Bei einem echten Einschalten des Mobiles und dem darauf folgenden Einbuchen würde die Tracezeile in Tafel 34

„0d 0000---- Location updating and the network sets NECI bit to 1“

lauten. Die Ursache besteht darin, dass der in Bild 31 dargestellte Trace durch Forcing (Manipulation) seitens des Programms OTDrive4 zustandegekommen ist, bei dem die Procedur des LOCATION UPDATE bei bereits eingebuchten Mobile wiederholt wird.

8.2.1 Die Meldung LOCATION UPDATING REQUEST

DieMeldung in Tafel 36 enthält eine Reihe bekannter IE, wie z.B. *Mobile Identity , Local area identification, Ciphering key sequence number.* Das IE *Mobile station classmark 1* wurde zwar noch nicht besprochen , aber es enthält auch keine neuen Elemente.

```
_____[ 227 ]___[ 18923 ]___[ UP ]___[ NAS ]_____________

05 08 12 62  f2 10 31 04  33 05 f4 87  16 b3 f0

05  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0101  Protocol Discrim.   : mobility management messages non GPRS
08  00------  SendSequenceNumber  : 0

    --001000  MESSAGE TYPE        : LOCATION UPDATING REQUEST

: Location updating type
12  ----0---  No follow-on request pending
    -----0--  Spare
    ------10  IMSI attach

: Ciphering key sequence number
    0-------  spare
    -001----  Ciph. Key Sequ.Numb.: 1

: Local area identification
62  ----0010  Mobile CC digit 1   : 2
    0110----  Mobile CC digit 2   : 6
f2  ----0010  Mobile CC digit 3   : 2

    1111----  Mobile NC digit 3   : 15
10  ----0000  Mobile NC digit 1   : 0
    0001----  Mobile NC digit 2   : 1

31  00110001  Loc. area code (LAI) = ID of MSC (hex)
04  00000100  Loc. area code (LAI) = ID of BSC (hex)


: Mobile station classmark 1
33  0-------  Spare
    -01-----  Revision Level      : Used by phase2 mobile stations
    ---1----  "Controlled Early Classmark Sending" option is implemented in the MS
    ----0---  encryption algorithm A5/1 available
    -----011  RF power capability : class4
```

```
: Mobile identity
05  00000101  length of Mob.ident.: 5

f4  1111----  Identity Digit 1    : 15
    ----0---  No. of ID digits    : even
    -----100  Type of identity    : TMSI/P-TMSI
87  10000111  Identity Digit 2,3  : take hex value
16  00010110  Identity Digit 4,5  : take hex value
b3  10110011  Identity Digit 6,7  : take hex value
f0  11110000  Identity Digit 8,9  : take hex value
```

Tafel 35: Inhalt einer Meldung LOCATION UPDATING REQUEST

Mit der Aufforderung *IMSI attach* im IE *Location updating type* wird erreicht, dass das Mobile im VLR als anwesend eingetragen wird, also mit PAGING REQUEST gerufen werden kann. Beim Ausschalten des Mobiles wird ein IMSI detach ausgeführt, das Mobile wird im VLR als nicht erreichbar eingetragen.
Durch diese Maßnahme wird ein aufwändiges Suchen des ausgeschalteten Mobiles im Netz durch PAGING REQUEST verhindert.

8.2.2 Die Meldungen AUTHENTICATION REQUEST und AUTHENTICATION RESPONSE

Im Bild 31 „Location Update“ werden sodann die Meldungen AUTHENTICATION REQUEST (Tafel 19) und AUTHENTICATION RESPONSE (Tafel 20) ausgetauscht. Das dabei angewandte Prinzip wurde bereits im Abschnitt 7.10.1 Über die Verschlüsselung des Transportkanals besprochen.

In der Bezeichnung der Meldungen liegt im Arbeitsblatt ein Fehler vor, es heißt gemäß ETS AUTHENTICATION und nicht AUTHENTIFICATION.

8.2.3 Die Meldung LOCATION UPDATING ACCEPT

Mit der Meldung LOCATION UPDATING ACCEPT (Tafel 36) übergibt das Netz den neuen Standort und die neue TMSI.

```
_____[ 193 ]___[ 19324 ]___[ DOWN ]___[ NAS ]_____________

05 02 62 f2  10 31 04 17  05 f4 87 16  f1 67

05  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0101  Protocol Discrim.   : mobility management messages non GPRS
02  00------  SendSequenceNumber  : 0

    --000010  MESSAGE TYPE        : LOCATION UPDATING ACCEPT

: Location area identification
62  ----0010  Mobile CC digit 1   : 2
    0110----  Mobile CC digit 2   : 6
f2  ----0010  Mobile CC digit 3   : 2

    1111----  Mobile NC digit 3   : 15
10  ----0000  Mobile NC digit 1   : 0
    0001----  Mobile NC digit 2   : 1

31  00110001  Loc. area code (LAI) = ID of MSC (hex)
04  00000100  Loc. area code (LAI) = ID of BSC (hex)


17  00010111  INFORMATIONSELEMET   : Mobile Identity 3

05  00000101  length of Mob.ident.3: 5
f4  1111----  Identity Digit 1     : 15
    ----0---  No. of ID digits     : even
    -----100  Type of identity     : TMSI/P-TMSI
87  1000----  Identity Digit 3     : 8
```

```
    ----0111  Identity Digit 2     : 7
16  0001----  Identity Digit 5     : 1
    ----0110  Identity Digit 4     : 6
f1  1111----  Identity Digit 7     : 15
    ----0001  Identity Digit 6     : 1
67  0110----  Identity Digit 9     : 6
    ----0111  Identity Digit 8     : 7
```

Tafel 36: Inhalt einer Meldung LOCATION UPDATING ACCEPT

8.2.4 Die Meldung TMSI REALLOCATION COMMAND

Es gibt außerhalb des *Location Updates* noch weitere Situationen in denen die TMSI erneuert wird. In der Meldung TMSI REALLOCATION COMMAND (Tafel 37) die beim Senden einer SMS eingesetzt wird ist außer der neuen TMSI nur noch der Standort im IE *Location area identification* . enthalten.

```
_____[ 107 ]___[ 506976 ]___[ DOWN ]___[ NAS ]_____________

05 1a 62 f2  10 36 0c 05  f4 07 99 25  f6

05  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0101  Protocol Discrim.   : mobility management messages non GPRS
1a  00------  SendSequenceNumber  : 0
    --011010  MESSAGE TYPE        : TMSI REALLOCATION COMMAND

: Location area identification
62  ----0010  Mobile CC digit 1   : 2
    0110----  Mobile CC digit 2   : 6
f2  ----0010  Mobile CC digit 3   : 2

    1111----  Mobile NC digit 3   : 15
10  ----0000  Mobile NC digit 1   : 0
    0001----  Mobile NC digit 2   : 1

36  00110110  Loc. area code (LAI) = ID of MSC (hex)
0c  00001100  Loc. area code (LAI) = ID of BSC (hex)

: Mobile identity
05  00000101  length of Mob.ident.: 5

f4  1111----  Identity Digit 1    : 15
    ----0---  No. of ID digits    : even
    -----100  Type of identity    : TMSI/P-TMSI
07  00000111  Identity Digit 2,3  : take hex value
99  10011001  Identity Digit 4,5  : take hex value
25  00100101  Identity Digit 6,7  : take hex value
f6  11110110  Identity Digit 8,9  : take hex value
```

Tafel 37: Inhalt einer Meldung TMSI REALLOCATION COMMAND

.
.
.

8.2.5 Die Meldung TMSI REALLOCATION COMPLETE

Die Bestätigung des Mobiles dass es seine alte TMSI gegen die neue ausgetauscht hat, erfolgt in der Meldung TMSI REALLOCATION COMPLETE.

```
.
_____[ 105 ]___[ 506976 ]___[ UP ]___[ NAS ]_____________

05 1b

05  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0101  Protocol Discrim.   : mobility management messages non GPRS
1b  00------  SendSequenceNumber  : 0
    --011011  MESSAGE TYPE        : TMSI REALLOCATION COMPLETE
```

Tafel 38: Inhalt einer Meldung TMSI REALLOCATION COMPLETE

9. Die Meldungen für die Rufsteuerung (Call Control)

Wer den Lehrbrief „Der ISDN-D-Kanal“ aufmerksam gelesen hat, wird in den nachstehenden Ausführungen viel Bekanntes finden
Schauen wir uns zunächst die auf Tafel 1 gegenüber gestellten Nachrichten für die unterschiedlichen Zweckbestimmungen an.

Meldung	DSS-1 Code	GSM Code, SSN-Code	UMTS	Bedeutung
SETUP	05	05,45	05,45	Einleiten des Verbindungsaufbaus
CALL CONFIRMED	-	08,48	08,48	MS bestätigt ankommenden Ruf
ALERTING	01	01,41	01,41	EE zur Annahme des Rufs bereit
CALL PROCEEDING	02	02,42	02,42	Netz benötigt keine Informationen mehr
CONNECT	07	07,47	07.47	Rufannahme wird bestätigt
CONNECT ACKNOW.	0F	0F,4F	0F,4F	Durchschaltung des B-Kanals im Netz
EMERGENCY SETUP	-	0E,4E	0E,4E	Notruf Anforderung
PROGRESS	03	03,43	03,43	Zeigt Verbindungsübergänge an
MODIFY	-	17,57	17,57	Forderung BC Wechsel
MODIFY COMPLETE	-	1f,5f	1f,5f	BC Wechsel Vollzug
MODIFY REJECT	-	13,53	13,53	BC Wechsel Fehler
USER INFORMATION	20	10,57	10,50	End-to-End Übertragung von Informationen
HOLD	24	18,58	18,58	Anforderung des Haltezustands für die Verbindung
HOLD ACKNOWL.	28	19,59	19,59	Positive Bestätigung für HOLD
HOLD REJECT	30	1a,5a	1a,5a	Abweisung des Holdbefehls
RETRIEVE	31	1c,5c	1c,5c	Forderung der Rückführung des Kanals aus Hold
RETRIEVE ACKNOWL.	32	1d,5d	1d,5d	Positive Bestätigung Retrieve
RETRIEVE REJECT	33	1e,5e	1e,5e	Abweisung d. Retrievebefefehls.
DISCONNECT	45	25,65	25,65	EE fordert Auslösung einer Verb. Netz zeigt Ausl.einer Verb.an
RELEASE	4D	2d,6d	2d,6d	Reaktion auf Disconnect (von EE: Freigabe des B-Kanals)
RELEASE COMPL.	5A	2a,6a	2a,6a	Quittung von Release, Freigabe von TI und B(m)-Kanal
SETUP ACKNOWLEDE	0D	-	-	TK-Anl. zeigt unvollständigen Ruf an
CONGESTION CTRL	-	39,79	39,79	Anzeige der Einrichtung oder Beendigung der Flusskontr..f.UI
NOTIFY	6e	3e,7e	3e,7e	Anzeige von Nachrichten die zur Verbindung gehören
STATUS	7d	3d,7d	3d,7d	Antwort.auf STATUS ENQUIRY
STATUS ENQUIRY	75	34,74	34,74	Anforderung einer Statusinform.
START DTMF	-	35,75	35,75	Anforderung der Wandlg von bits in DTMF
STOP DTMF	-	31,71	31,71	Beendigung der Wandlung von bits in DTMF
STOP DTMF ACK.	-	32,72	32,72	Akzeptanz von STOP DTMF
START DTMF ACK.	-	36,76	36,76	Akzeptanz von START DTMF
START DTMF REJ.	-	37,77	37,77	Zurückweisg, von START DTMF
FACILITY	62	3a,7a	3a,7a	Anforderung eines (verbindungsabhängigen) Dienstmerkmals

Tabelle 1 : CC-Messages im ISDN und im Mobilfunk. Für unterstrichene Meldungen existierren Trace.

Man erkennt, dass in vielen Fällen sogar die Kodierung der Meldungen in DSS1, GSM und UMTS übereinstimmt.
Die Mobilfunktechnischen Besonderheiten sollen anhand von Tracen in den nachstehenden Beispielen besprochen werden.

Beginnen wir mit der Meldung SETUP. Es muss zwischen der Meldung SETUP die vom ISDN zum Mobile gesendet wird (MTC) und der, die das Mobile ins Netz sendet. (MOC) unterschieden werden.

9.1 Die Meldung SETUP

Der Inhalt der Meldung SETUP (Tafel 39) des MTC ähnelt sehr stark dem im ISDN. Man findet die Bearer capability, die Calling Party Number und die High Layer Compatibility.

```
_____[ 399 ]___[ 1261908 ]___[ DOWN ]___[ NAS ]_____________

13 05 04 01  a0 5c 08 11  81 94 33 57  92 28 f1 7d  02 91 81

13  0-------  direction from      : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
05  00------  SendSequenceNumber  : 0

    --000101  MESSAGE TYPE        : SETUP

04  00000100  INFORMATION ELEMENT : Bearer capability
01  00000001  length              : 1
a0  1-------  Extension           : 1
    -01-----  Radio Channel Req.  : full rate support only MS
    ---0----  Coding Standard     : GSM standard coding
    ----0---  Transfer Mode       : Circuit Mode
    -----000  Info Transfer Cap.  : speech

5c  01011100  INFORMATION ELEMENT : Calling party BCD number
08  00001000  length              : 8
11  0-------  Extension           : 0
    -001----  Type of number      : international number
    ----0001  Numb. plan id.      : ISDN/telephony numb. pl. (Rec. E.164/E.163)
81  1-------  Extension           : 1
    -00-----  Present.indic.      : Presentation allowed
    ---000--  spare               : 0
    ------01  Present.indic.      : User-provided, verified and passed
94..f1        number              : 49337529821

7d  01111101  INFORMATION ELEMENT : High Layer Compatibility
02  00000010  length              : 2
91  1-------  Extension           : 1
    -00-----  Coding standard     : CCITT standardized coding
    ---100--  Interpret.i.ch.     : First high layer char.id. to be used
    ------01  Present.method      : High Layer protocol profile
81  10000001  High layer char.    : Telephony
```

Tafel 39: Inhalt einer Meldung SETUP im *Mobile Terminated Call* MTC

Im Unterschied zum ISDN existiert die Möglichkeit zwei Bearer capability IE, zwei High layer compatibility IE und zwei Low layer compatibility IE anzugeben. Das rührt daher, dass man einen Ruf mit einem Dienst aufbauen kann (z.B. Sprache) um während des Gesprächs einen Dienstwechsel (z.B. zu FAX) vorzunehmen. So etwas ist nicht neu, ein Informationselement Dienstwechsel gab bereits im Protokoll 1TR6 im nationalen ISDN. Dem Verfasser ist jedoch kein Mobile bekannt, das diesen Dienstwechsel unterstützt. Es müsste dann eine Taste oder ein Softkey vorhanden sein, der die Meldung MODIFY zum Einleiten des Dienstwechsels aussendet.
Weitere Informationselemente im SETUP des MTC können sein: die IE *BC repeat indicator*, *Facility, Signal, Progressindikator, Signal, Calling Party Subaddress, Called party BCD number Called party subaddress, Redirecting party BCD number, Redirecting party subaddress, LLC repeat indicator*, *Low Layer Compatibility, HLC repeat indicator, Priority* und *User-user* möglich. Alle diese IE sind aus dem ISDN bekannt.

Beim MOC fehlen die in der Aufzählung unterstrichenen IE in der SETUP Meldung, da sie nur vom Netz generiert werden können.
Es können jedoch Informationselemente enthalten sein, die sich auf Supplementary Services beziehen wie *SS version indicator, CLIR suppression, CLIR invocation* oder
FACILITY $(CCBS)$. Diese IE gibt es im ISDN nicht. Wir werden bei der Besprechung der Dienstmerkmale darauf zurückkommen.

Der Inhalt des IE *Bearer capability* in der MOC SETUP Meldung ist offenbar auch nicht konform mit dem Inhalt des Bearer im ISDN. So werden z.B. die vom Mobile unterstützten Versionen der Sprachkodierung (S*peech version indicator)* angegeben.

```
_____[ 269 ]___[ 4534068 ]___[ UP ]___[ NAS ]_____________

03 85 04 06  60 04 02 00  05 81 5e 07  91 94 33 57  92 28 f1

03  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0011  Protocol Discrim.   : Call control and call related SS messages
85  10------  SendSequenceNumber  : 0

    --000101  MESSAGE TYPE        : SETUP

04  00000100  INFORMATION ELEMENT : Bearer capability
06  00000110  length              : 6
60  0-------  Extension           : 0
    -11-----  Radio Channel Req.  : dual rate support MS/full rate preferred
    ---0----  Coding Standard     : GSM standard coding
    ----0---  Transfer Mode       : Circuit Mode
    -----000  Info Transfer Cap.  : speech
04  0-------  Extension           : 0
    -0------  Coding              : octet used for extension of inf. transf. capab.
    --00----  Spare               : 00
    ----0100  speech Vers. indic. : GSM full rate speech version 3
02  0-------  Extension           : 0
    -0------  Coding              : octet used for extension of inf. transf. capab.
    --00----  Spare               : 00
    ----0010  speech Vers. indic. : GSM full rate speech version 2
00  0-------  Extension           : 0
    -0------  Coding              : octet used for extension of inf. transf. capab.
    --00----  Spare               : 00
    ----0000  speech Vers. indic. : GSM full rate speech version 1
05  -0------  Compression         : data compression not possible
    --00----  Structure           : service data unit integrity
    ----0---  Duplex Mode         : half duplex
    ------0-  Negot. of Int.      : No meaning is associated with this value.
81  1-------  Extension           : 1
    -00-----  Access ID           : octet identifier
    ---00---  Rate Adaptation     : no rate adaption
    -----001  Signalling Acc.Prot : I.440/450

5e  01011110  INFORMATION ELEMENT : CalledPartyBCDNumber
07  00000111  length              : 7
91  1-------  Extension           : 1
    -001----  Type of number      : international number
    ----0001  Numb. plan id.      : ISDN/teleph. numb. plan (Rec. E.164/E.163) _
94..f1        number              : 49337529821
```

Tafel 40: Inhalt einer Meldung SETUP im *Mobile Originated Call* MOC

Das muss so sein, weil durch die Angabe des Bearer dem Netz mitgeteilt wird , was man von der Schicht 1 im Netz für Übertragungseigenschaften erwartet werden. Diese sind natürlich durch die Sprachkompression andere als die im ISDN.

Trotzdem besteht eine Besonderheit im GSM gegenüber dem ISDN. Das Informationselement *Bearer capability* ist im ISDN Pflichtelement, im GSM ist es das nicht.

Betrachten Sie bitte dazu das SETUP eines MTC in Tafel 41

Bei einem Versuch zum Mobile OT 460 aus dem ISDN mit FRITZ!data eine Datenverbindung aufzubauen, kam der Ruf im Mobile nicht an. Im ISDN gab es die Fehlermeldung „Übermittlungseigenschaft (Bearer Capability) nicht zugelassen“.

```
_____[ 63 ]___[ 391267 ]___[ DOWN ]___[ NAS ]_____________

13 05 5c 08  11 83 94 33  57 92 28 f1

13  0-------  direction from      : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
05  00------  SendSequenceNumber  : 0

    --000101  MESSAGE TYPE        : SETUP

5c  01011100  INFORMATION ELEMENT : Calling party BCD number
08  00001000  length              : 8
11  0-------  Extension           : 0
    -001----  Type of number      : international number
    ----0001  Numb. plan id.      : ISDN/telephony numb. pl. (Rec. E.164/E.163)
83  1-------  Extension           : 1
    -00-----  Present.indic.      : Presentation allowed
    ---000--  spare               : 0
    ------11  Present.indic.      : Network provided
94..f1        number              : 49337529821
```

Tafel 41: Inhalt einer Meldung SETUP im *Mobile* MTC einer unberechtigten DFÜ-Verbindung

Es ist notwendig Datenübertragung im GSM beim Operator zu beauftragen. Man bekommt mit der Beauftragung eine spezielle Mobile-Nummer mit der DFÜ möglich ist. Das erfordert den Abschluss eines besonderen Tarifes.

9.2 Die Meldung CALL CONFIRMED

Das SETUP wird quittiert von der Meldung CALL CONFIRMED (Tafel 42). Diese Meldung enthält den BEARER, teilt dem Netz also mit, was das Mobile kann. Das Netz (das MSC oder das G-MSC) kann daher die Angaben des BEARER des aus dem ISDN (Fernnetz) ankommenden SETUP mit den Angaben aus der Meldung CALL CONFIRMED vergleichen. Stellt es Nichtübereinstimmung fest erzeugt es die o.a. Fehlermeldung.

```
_____[ 397 ]___[ 1261908 ]___[ UP ]___[ NAS ]_____________

93 88 04 06  60 04 02 00  05 81

93  1-------  direction to        : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
88  10------  SendSequenceNumber  : 0

    --001000  MESSAGE TYPE        : CALL CONFIRMED

04  00000100  INFORMATION ELEMENT : Bearer capability
06  00000110  length              : 6
60  0-------  Extension           : 0

    -11-----  Radio Channel Req.  : dual rate support MS/full rate preferred
    ---0----  Coding Standard     : GSM standard coding
    ----0---  Transfer Mode       : Circuit Mode
    -----000  Info Transfer Cap.  : speech
04  0-------  Extension           : 0
    -0------  Coding              : octet used for extension of inf. transf. capab.
    --00----  Spare               : 00
    ----0100  speech Vers. indic. : GSM full rate speech version 3
02  0-------  Extension           : 0
    -0------  Coding              : octet used for extension of inf. transf. capab.
    --00----  Spare               : 00
    ----0010  speech Vers. indic. : GSM full rate speech version 2
00  0-------  Extension           : 0
    -0------  Coding              : octet used for extension of inf. transf. capab.
```

```
    --00----  Spare               : 00
    ----0000  speech Vers. indic. : GSM full rate speech version 1
05  -0------  Compression         : data compression not possible
    --00----  Structure           : service data unit integrity
    ----0---  Duplex Mode         : half duplex
    ------0-  Negot. of Int.      : No meaning is associated with this value.
81  1-------  Extension           : 1
    -00-----  Access ID           : octet identifier
    ---00---  Rate Adaptation     : no rate adaption
    -----001  Signalling Acc.Prot : I.440/450
```

Tafel 42: Inhalt einer Meldung CALL CONFIRMED

Das aus dem ISDN bekannte Prinzip, dass der Dienst im BEARER formuliert wird bleibt somit bestehen, nur ist der Mechanismus der Überprüfung der Angaben geändert.

9.3 Die Meldung ALERTING

Nun folgt analog den Regeln des ISDN die Meldung ALERTING, in Tafel 43 ohne zusätzliches IE.

```
_____[ 377 ]___[ 1262176 ]___[ UP ]___[ NAS ]_____________

93 c1

93  1-------  direction to        : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
c1  11------  SendSequenceNumber  : 1

    --000001  MESSAGE TYPE        : ALERTING
```

Tafel 43: Inhalt einer Meldung ALERTING im MTC

Es ist zu unterscheiden ob die Meldung ALERTING vom Netz ausgesendet wird oder vom Mobile. Das ALERTING im MTC s.o. kann optional noch die IE *Facility*, *User-user* und *SS version* enthalten. Das ALERTING im MOC (Tafel 44) enthält hier den *Progress indicator* und könnte optional noch die IE *Facility* und *User-user* beinhalten.

```
_____[ 211 ]___[ 4534910 ]___[ DOWN ]___[ NAS ]_____________

83 01 1e 02  ea 88

83  1-------  direction to        : originating site
    -000----  TransactionID       : 0
    ----0011  Protocol Discrim.   : Call control and call related SS messages
01  00------  SendSequenceNumber  : 0

    --000001  MESSAGE TYPE        : ALERTING

1e  00011110  INFORMATION ELEMENT : Progress indicator
02  00000010  L. OF IE PROG.IND.  : 2
ea  1-------  Extension           : 1
    -11-----  Coding standard     : Stand. Def. for the GSM-PLMNS as descry.
    ---0----  Spare               : 0
    ----1010  Location            : Network beyond interworking point
88  1-------  Extension           : 1
    -0001000  Progress descr.     : In-band inform. or appr. pattern now available
```

Tafel 44: Inhalt einer Meldung ALERTING im MOC

9.4 Die Meldung CONNECT

Die Meldung CONNECT im MTC (Tafel 45) besitzt ebenfalls kein Informationselement, jedoch sind gemäß ETS wieder optionale IE möglich.

```
_____[ 333 ]___[ 1263229 ]___[ UP ]___[ NAS ]_____________

93 07

93  1-------  direction to        : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
07  00------  SendSequenceNumber  : 0

    --000111  MESSAGE TYPE        : CONNECT
```

Tafel 45: Inhalt einer Meldung CONNECT im MTC

Im MTC sind es die *IE Facility, Progress indicator, Connected number, Connected subaddress* und *User-user,* wie wir es aus dem ISDN gewohnt sind.
Im MOC sind es die *IE Facility, Connected subaddress* , *User-user* und *SS version indicator.*

9.5 Die Meldung CONNECT ACKNOWLEDGE

Die Meldung CONNECT ACKNOWLEDGE enthält in beiden Richtungen keine optionalen Elemente.

```
_____[ 325 ]___[ 1263290 ]___[ DOWN ]___[ NAS ]_____________

13 0f

13  0-------  direction from      : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
0f  00------  SendSequenceNumber  : 0

    --001111  MESSAGE TYPE        :CONNECT ACKNOWLEDGE
```

Tafel 46: Inhalt einer Meldung CONNECT ACKNOWLEDGE

.

9.6 Die Meldung DISCONNECT

Das IE *Cause* ist in DISCONNECT Pflichtelement Die Liste der möglichen Gründe ist in Tafel 47 enthalten. Sie ist ähnlich umfangreich wie im ISDN, zeigt den Ort des Auftretens eines Ereignisses und lässt dadurch auch eine detaillierte Diagnose zu.

```
0-------  Extension Bit       : 0
1-------  Extension Bit       : 1
-00-----  Coding stand.       : Coding as specified in CCITT Rec. Q.931
-01-----  Coding stand.       : Reserved for other international standards
-10-----  Coding stand.       : National standard
-11-----  Coding stand.       : Standard defined for the GSM-PLMNS
---0----  spare               : 0
----0000  location            : user
----0001  location            : private network serving the local user
```

```
----0010  location           : public network serving the local user
----0011  location           : transit network
----0100  location           : public network serving the remote user
----0101  location           : private network serving the remote user
----0111  location           : international network
----1010  location           : network beyond interworking point

-0000001  cause              : Unassigned (unallocated) number
-0000011  cause              : No route to destination
-0000110  cause              : Channel unacceptable
-0001000  cause              : Operator determined barring
-0010000  cause              : Normal call clearing
-0010001  cause              : User busy
-0010010  cause              : No user responding
-0010011  cause              : User alerting, no answer
-0010101  cause              : Call rejected
-0010110  cause              : Number changed, New destination
-0011001  cause              : Pre-emption
-0011010  cause              : Non selected user clearing
-0011011  cause              : Destination out of order
-0011100  cause              : Invalid number format (incomplete number)
-0011101  cause              : Facility rejected
-0011110  cause              : Response to STATUS ENQUIRY
-0011111  cause              : Normal, unspecified
-0100010  cause              : No circuit/channel available
-0100110  cause              : Network out of order
-0101001  cause              : Temporary failure
-0101010  cause              : Switching equipment congestion
-0101011  cause              : Access information discarded
-0101100  cause              : requested circuit/channel
-0101111  cause              : Resources unavailable, unspecified
-0110001  cause              : Quality of service unavailable
-0110010  cause              : Requested facility not subscribed
-0110111  cause              : Incoming calls barred within the CUG
-0111001  cause              : Bearer capability not authorized
-0111010  cause              : Bearer capab. not presently available
-0111111  cause              : Service or option not avail.unspecified
-1000001  cause              : Bearer service not implemented
-1000100  cause              : ACM equal to or greater than ACMmax
-1000101  cause              : Requested facility not implemented
-1000110  cause              : Only restricted dig. Inform. bearer capability is available.
-1001111  cause              : Service or option not implemented, unspecified
-1010001  cause              : Invalid transaction identifier value
-1010111  cause              : User not member of CUG
-1011000  cause              : Incompatible destination Incompatible parameter
-1011011  cause              : Invalid transit network selection
-1011111  cause              : Semantically incorrect message
-1100000  cause              : Invalid mandatory information
-1100001  cause              : Message type non-existent or not implemented
-1100010  cause              : Message type not compatible with protocol state
-1100011  cause              : Information element non-existent or not implemented
-1100100  cause              : Conditional IE error
-1100101  cause              : Message not compatible with  protocol state
-1100110  cause              : Recovery on timer expiry
-1101111  cause              : Protocol error, unspecified
-1111111  cause              : Interworking, unspecified
```

Tafel 47: Werte die das Informationselement CAUSE annehmen kann

```
_____[ 294 ]___[ 1264027 ]___[ DOWN ]___[ NAS ]_____________

13 25 02 e0  90

13  0-------  direction from      : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
25  00------  SendSequenceNumber  : 0

    --100101  MESSAGE TYPE        : DISCONNECT

02  00000010  LENGTH OF IE CAUSE  : 2
e0  1-------  Extension Bit       : 1
    -11-----  Coding stand.       : Standard defined for the GSM-PLMNS
    ---0----  spare               : 0
```

```
    ----0000  location            : user
90  -0010000  cause               : Normal call clearing
```

Tafel 48: Inhalt einer Meldung DISCONNECT im MTC

Weiter optionale IE sind *Facility, User-user* und *Allowed actions*. Das Letztere wird im Zusammenhang mit dem Dienstmerkmal CCBS (Rückruf bei besetzt) eingesetzt.
Die Meldung DISCONNECT im MOC enthält optional *Facility, User-user* und *SS version*. Letzteres wird verwendet, um bei Vorhandensein des IE Facility die Version (den Entwicklungsstand) des Supplementary Service anzuzeigen.

9.7 Die Meldung RELEASE

Die Meldung RELEASE (Tafel 49) enthält hier nicht das Informationselement *cause,* den Grund für die Freigabe des Kanals durch das Netz.

```
_____[ 292 ]___[ 1264027 ]___[ UP ]___[ NAS ]_____________

93 6d

93  1-------  direction to        : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
6d  01------  SendSequenceNumber  : 1

    --101101  MESSAGE TYPE           : RELEASE
```

Tafel 49: Inhalt einer Meldung RELEASE

Gemäß GSM 04.08 kann RELEASE im MTC optional die IE *Cause, Facility* und *User-user* enthalten, sowie noch eine zweites IE *Cause.*
In einer (in GSM 04.08) bestimmten Situation kann nämlich sowohl der Grund für ein vorausgegangenes DISCONNECT als auch der, davon verschiedene, Grund für das nachfolgend RELEASE angezeigt werden. Im MOC kann noch das IE *SS version* enthalten sein

9.8 Die Meldung RELEASE COMPLETE

Die Meldung RELEASE COMPLETE (Tafel 50) enthält das Informationselement *Cause*.
RELEASE COMPLETE im MTC kann desweiteren die Informationselemente *Facility* und *User-user* enthalten. Im MOC kann noch das IE *SS version* enthalten sein
Wie bei der Besprechung der Dienstmerkmale zu sehen ist, wird RELEASE COMPLETE als Antwort des Netzes auf die Meldung FACILITY REGISTER zusammen mit dem IE *Facility* verwendet.

```
_____[ 288 ]___[ 1264092 ]___[ DOWN ]___[ NAS ]_____________

13 2a 08 02  e0 90

13  0-------  direction from      : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
2a  00------  SendSequenceNumber  : 0

    --101010  MESSAGE TYPE        : RELEASE COMPLETE

08  00001000  INFORMATION ELEMENT : Cause
02  00000010  LENGTH OF IE CAUSE  : 2
e0  1-------  Extension Bit       : 1
    -11-----  Coding stand.       : Standard defined for the GSM-PLMNS
    ---0----  spare               : 0
```

```
    ----0000  location            : user
90  -0010000  cause               : Normal call clearing
```

Tafel 50: Inhalt einer Meldung RELEASE COMPLETE

10. Dienste im GSM

Nachstehend werden Trace aus Messungen vorgestellt, die mit der Messanordnung in Bild 37 gefangen wurden.

Damit der interessierte Leser mit wenig finanziellem Aufwand selbst Messungen durchführen kann, wird die Installation der nachstehen Messanordnung empfohlen:

- Sie benötigen ein normales Mobile das mit einem dazu gelieferte Kabel mit einem PC verbunden werden kann. Die Verbindung des Mobiles mit dem PC wird für die Eingabe von AT-Befehlen benötigt, oder die Nutzung von Nobbis GSM-monitor
- Als ISDN-Komponente ist eine FRITZ!Card ISDN (entweder als PCI, PCMCIA oder als USB Version) erforderlich . Wenn Sie eine derartige Hardware bereits besitzen, sollten Sie die Software auf den Stand Version 3,08 oder neuer updaten.
- Desweiteren ist erforderlich sich von der Site www.shamrock.de -> Tools -> CAPIDOG als Freeware herunterzuladen Sie erhalten dann CAPIDOG Version 1.46 . Diese Version zeichnet die Signale der Schichten 2 und 3 des ISDN-D-Kanals auf. Capidog übersetzt den ISDN-D-Kanal String teilweise (vollständig tun das TraceView [5] und ISDNView [6]) sodass man zumindest einige Hauptparameter ablesen kann.
- Die Anordnung entspricht der in Bild 37, mit der Einschränkung, dass keine GSM-Dm-Trace aufgezeichnet werden.

Texte die sich auf diese Versuchsanordnung beziehen sind eingerahmt.

In [5] ist einen CD enthalten in der Trace der GSM-Dm-Kanäle und der ISDN-D-Kanäle von Übungen mit Diensten und Dienstmerkmalen gespeichert sind. Mit den ebenfalls enthaltenen Übersetzern GSMView und Traceview können Die Übungen nachvollzogen werden.

Das neueste SAGEM Tracemobile OT 460 wird mit [6] ausgeliefert. Dazu die Übersetzer EDGEView und ISDNView. Beide arbeiten interpretativ, d.h.sie übersetzen die Hexstrings der Trace anhand von ETSI konformen Scripten. Die CBT enthält eine Anleitung selbst Scripte herzustellen.

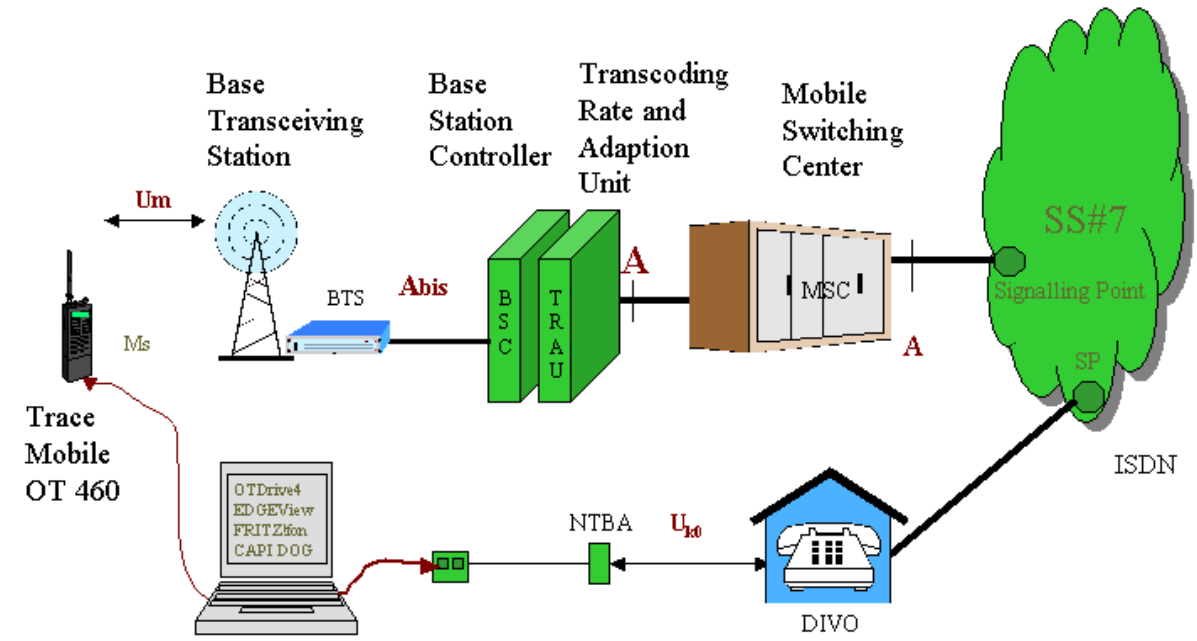


Bild 37: Messanordnung zum Untersuchen von Fernmeldeverbindungen zwischen ISDN und GSM

10.1 Fernsprechen

Das SETUP im MTC (Tafel 39) stammt aus einer Verbindung zwischen Mobile und ISDN. Der Bearer im SETUP ist ISDN-typisch er enthält *speech* als Dienst. Auch ist das Informationselement HLC mit dem Dienst Telephonie vorhanden
Im MOC (Tafel 40) verlangt das Mobile einen Sprachkanal, gibt seine Kompressionsmöglichkeiten an, was im ISDN einwandfrei als Telephonie gewertet wird,

Es ist von Interesse zu wissen, wie lange es dauert bis eine Verbindung vom Mobile ins Netz oder umgekehrt durchgeschaltet wird. Dazu wird in einem MOC die Zeitmarke des SETUP kontrolliert (34170) und danach die Zeitmarke der Rückmeldung aus dem ISDN, des ALERTING (34910) . Die Differenz 740 wird mit der Dauer eines TDMA-Rahmens (4,615 ms) multipliziert. Das Ergebnis ist 3,415 Sekunden.

Der Leser der die vorgeschlagene Versuchsanordnung mit Capidog aufgebaut hat, kann den Versuch von der ISDN-Seite aus durchführen und sein Mobile anrufen. Sobald das Mobile klingelt, kann der Versuch abgebrochen werden. Die Zeitdifferenz zwischen SETUP und eintreffenden ALERTING ist in etwa die Zeit in der der MTC aufgebaut wird.

10.2 Fax-Übertragung

Es sei nochmal daran erinnert, dass es bei FAX-Übertragungen im ISDN Kompatibilitätsproblemen gibt. Wenn die Faxsendestelle im SETUP ein HLC IE mit Inhalt „FAX G2/G3“ überträgt, kann diese Sendung nur zu einer Gegenstelle übertragen werden, die ebenfalls als ISDN-Fax eingestellt ist. Ein Faxgerät am Analoganschluss kann, weil es telephonietypisch angeschlossen ist, diese Sendung nicht empfangen. Das gleiche gilt umgekehrt.
In der Praxis werden daher Faxgeräte meist wie Analogtelefone angeschlossen. Damit Telefonie und Faxübertragung auseinander gehalten werden kann, wird, wenn nur eine Telefonnummer für beide zur Verfügung steht, eine Faxweiche eingesetzt. Eleganter ist die Verwendung getrennter Telefonnummern.

10.2.1. Faxen zum Mobile: Das Informationselement *High Layer Capability* zeigt Fax an

Im Mobilfunk liegen ähnliche Verhältnisse vor. In Tafel 51 ist das SETUP in einem MTC dargestellt, wenn die Gegenstelle im ISDN ein Faxgerät ist, das auf ISDN-Fax eingestellt ist. (In FRITZ!fax klickt man FRITZ!fax-Einstellungen->ISDN->Erweiterte Einstellungen->ISDN-Fax).

```
_____[ 6 ]___[ 215059 ]___[ DOWN ]___[ NAS ]_____________

13 05 04 07  a3 b8 81 20  15 63 80 5c  08 11 83 94  33 57 92 28
f1 7d 02 91  84
13  0-------  direction from      : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
05  00------  SendSequenceNumber  : 0

    --000101  MESSAGE TYPE        : SETUP

04  00000100  INFORMATION ELEMENT : Bearer capability
07  00000111  length              : 7
a3  1-------  Extension           : 1
    -01-----  Radio Channel Req.  : full rate support only MS
    ---0----  Coding Standard     : GSM standard coding
    ----0---  Transfer Mode       : Circuit Mode
    -----011  Info Transfer Cap.  : facsimile group 3
b8  1-------  Extension           : 1
    -0------  Compression         : data compression not possible
    ----1---  Duplex Mode         : full duplex
    -----0--  Configuration       : point-to-point
    ------0-  Negot. of Int.      : No meaning is associated with this value.
    -------0  Establishment       : demand
81  1-------  Extension           : 1
    -00-----  Access ID           : octet identifier
    ---00---  Rate Adaptation     : no rate adaption
    -----001  Signalling Acc.Prot : I.440/450
20  0-------  Extension           : 0
    -01-----  Layer 1 ID
    ---0000-  User Info L1 Prot   : Default layer1 protocol
    -------0  Sync/async          : synchronous
15  0-------  Extension           : 0
    -0------  Numb Stop Bits      : 1 bit (also used in the case of synchr mode)
    --0-----  Negotiation         : in-band negotiation not possible
    ---1----  Numb Data Bits      : 8 bits (also used i case of bit oriented protocols)
    ----0101  User Rate           : 9.6 kbit/sRecommendation X.1 and V.110
63  0-------  Extension           : 0
    -11-----  Intermediate Rate   : 16 kbit/s
    ---0----  NIC On Tx           : not require to send data with network  indep.clock
    ----0---  NIC On Rx           : can't accept data with network indep. clock
    -----011  Parity              : none
80  1-------  Extension           : 1
    -00-----  Connect Element     : transparent
    ---00000  Modem Type          : none
5c  01011100  INFORMATION ELEMENT : Calling party BCD number
08  00001000  length              : 8
11  0-------  Extension           : 0
    -001----  Type of number      : international number
    ----0001  Numb. plan id.      : ISDN/telephony numb. pl. (Rec. E.164/E.163)
83  1-------  Extension           : 1
    -00-----  Present.indic.      : Presentation allowed
    ---000--  spare               : 0
    ------11  Present.indic.      : Network provided
94..f1        number              : 49337529821
7d  01111101  INFORMATION ELEMENT : High Layer Compatibility
02  00000010  length              : 2
91  1-------  Extension           : 1
    -00-----  Coding standard     : CCITT standardized coding
    ---100--  Interpret.i.ch.     : First high layer char.id. to be used
    ------01  Present.method      : High Layer protocol profile
84  10000100  High layer char.    : Facsimile Group 2/3
```

Tafel 51: SETUP eines MTC wenn die Gegenstelle ein ISDN-Fax ist

Im Bearer findet mann folgerichtig den Eintrag„*facsimile group 3*" und High Layer den Vermerk „*Facsimile Group 2/3*".
Die Meldung CALL CONFIRMED in Tafel 52 besitzt in diesem Fall kein Informationselement,

```
_____[ 5 ]___[ 215059 ]___[ UP ]___[ NAS ]_____________

93 88

93  1-------  direction to        : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
88  10------  SendSequenceNumber  : 0

    --001000  MESSAGE TYPE        : CALL CONFIRMED
```

Tafel 52: Die Meldung CALL CONFIRMED in einem MTC mit ISDN-Fax

Im MTC ist zwar ein ALERTING vorhanden, aber kein CONNECT!! Wohl aber ein DISCONNECT als Antwort auf das CHANNEL RELEASE vom Netz.

Man muss hier zwei Fälle unterscheiden: Der GSM-Teilnehmer hat den Dienst Fax mit seinem Mobile beautragt oder nicht:

- Der Dienst ist nicht beauftragt. Der Ruf kommt beim Mobile an, aber Sie können ihn nicht annehmen. Sie bekommen ggf. die Möglochkeit den Softkey „User busy" zu betätigen.
- Der Dienst ist beauftragt. Das Mobile klingelt, Man kann aber das Gespräch nicht annehmen (Das Drücken der grünen Taste bleibt wirkungslos). Das Fax wird vom Netz in die Mailbox geleitet, da das Mobile selbst das Fax nicht darstellen kann. Z.B. an ein Fax mit Bildern. Man erhält von der Mailbox einen Anruf. Es wird die Telefonnummer eines Faxgerätes erfragt auf dem das Fax wiedergegeben werden kann.

Der Leser der die vorgeschlagene Versuchsanordnung mit Capidog aufgebaut hat, kann einen Versuch von der ISDN-Seite aus durchführen und mit FRITZ!fax (Einstellung ISDN-Fax) sein Mobile anrufen. Das Ergebnis ist davon abhängig ob er den Dienst beauftragt hat oder nicht.

10.2.2. Faxen zum Mobile: Das Informationselement *Bearer Capability* im ISDN zeigt 3,1kHz audio an

```
_____[ 15 ]___[ 276001 ]___[ DOWN ]___[ NAS ]_____________

13 05 5c 08  11 83 94 33  57 92 28 f1

13  0-------  direction from      : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
05  00------  SendSequenceNumber  : 0

    --000101  MESSAGE TYPE        : SETUP
5c  01011100  INFORMATION ELEMENT : Calling party BCD number
08  00001000  length              : 8
11  0-------  Extension           : 0
    -001----  Type of number      : international number
    ----0001  Numb. plan id.      : ISDN/telephony numb. pl. (Rec. E.164/E.163)
83  1-------  Extension           : 1
    -00-----  Present.indic.      : Presentation allowed
    ---000--  spare               : 0
    ------11  Present.indic.      : Network provided
94..f1        number              : 49337529821
```

Tafel 53: SETUP im MTC bei Empfang eines Analog-Fax Aufruf.

In Tafel 53 ist das SETUP in einem MTC dargestellt, wenn ein Analog-Fax anruft.

Der BEARER sieht in diesem Fall aus wie bei einem Telefonat. Deshalb kann man das Gespräch auch annehmen. Man finde CONNECT im Trace, und auch DISCONNECT auf der Schicht 3.
Das Fax geht ins Leere, d.h. es wird nicht wiedergegeben..

Mit der vorgeschlagene Versuchsanordnung führt der Versuch von der ISDN-Seite aus, bei Einstellung Analog-Fax, zum Klingeln des Mobiles. Das „Gespräch“ kann angenommen, aber es kann (natürlich) nicht gesprochen werden.

Es gibt ein Lösung des Operators D1. Wenn man ein Mobile erwirbt und die Dienste Fax und Daten beauftragen, dann erscheint im Directory zusätzlich ein Menüpunkt **T-D1 Special** mit dem Unterpunkt Mail&Fax und darunter Fax Versand. Ein derartiges Fax wird als SMS versendet.

```
05 24 64 03 23 19 01 05 f4 64 ad f9 11

05  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0101  Protocol Discrim.   : mobile management messages non GPRS
24  00------  SendSequenceNumber  : 0

    --100100  MESSAGE TYPE        : CM SERVICE REQUEST

64  0-------  spare               : 0
    -110----  value for the ciphering key sequence number = 6
    ----0100  Requ.service type   : Short message service

: Mobile Station Classmark 2
03  00000011  length              : 3

23  0-------  1 spare             : 0
    -01-----  Revision Level      : Used by phase 2 mobile stations
    ---0----  "Controlled Early Classmark Sending" option is not implemented in the MS
    ----0---  Encryp.Algor. A5_1  : available
    -----011  RF power capability : Class 4, handheld

19  0-------  1 spare bit         : 0
    -0------  pseudo-synch.capab. : not present
    --01----  SS Screening Indic. : phase 2 error handling
    ----1---  Mobile station supports mobile terminated point to point SMS
    -----0--  no VoiceBroadcastService (VBS) capability or no notifications wanted
    ------0-  no VoiceGroupCallService (VGCS) capability or no notifications wanted
    -------1  The MS does support the E-GSM or R-GSM

01  0-------  The MS does not support any options that are indicated in CM3
    -0------  1 spare bit         : 0
    --0-----  LocationServiceValueAdded Capability  not supported
    ---0----  1 spare bit         : 0
    ----0---  SoLSA Capability    : not supported
    -----0--  Network initiated MO CM connection request not supported.
    ------0-  encryp.algorith.A5/3: not available
    -------1  encryp.algorith.A5/2: available

: Mobile identity

05  00000101  length              : 5

f4  ----0---  No. of ID digits     : even
    -----100  Type of identity     : TMSI/P-TMSI
    1111----  Identity Digit 1     : 95
64  01100100  Identity Digit 2,3   : take hex value
ad  10101101  Identity Digit 4,5   : take hex value
f9  11111001  Identity Digit 6,7   : take hex value
11  00010001  Identity Digit 8,9   : take hex value
```

Tafel 54: In der Betriebsart Mail&Fax bei D1 wird das Fax als SMS verschickt

Im Trace findet man kein SETUP, aber in der Meldung CM SERVICE REQUEST steht als *Requested service type* „Short message service“. D.h. das Fax wird als SMS übertragen

10.2.3. Faxen vom Mobile ins GSM

Das Faxen von Mobile zu Mobile funktioniert genauso, nur dass das Fax wieder in der Mailbox zwischengelagert und dann an ein definiertes Faxgerät im Festnetz übertragen wird,

Schlussfolgerung:
Sieht man von der Verwendung der SMS bei Fax vom Mobile ab, so gilt das im Zusammenhang mit dem ISDN erarbeitete, dass der Dienst *facsimile Group 2/3* im Informationselement HLC angegeben sein muss damit das Netz den Faxdienst akzeptiert.

10.3 Datenübertragung

10.3.1 Datenübertragung im GSM ist nicht beauftrag

In Tafel 41 ist der Inhalt einer Meldung SETUP im MTC einer unberechtigten DFÜ-Verbindung dargestellt. Eine derartiges SETUP findet man im Trace eines OT 460 wenn man es mit FRITZ!data anruft und der Dienst Datenübertragung nicht beauftragt ist. Wenn auch das SETUP keinen BEARER besitzt, so meldet doch die Message CALL CONFIRMED dem Netz welche Übertragungs-eigenschaften das Mobile besitzt.

```
_____[ 49 ]___[ 299485 ]___[ UP ]___[ NAS ]_____________

93 08 04 06  60 04 02 00  05 81

93  1-------  direction to        : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
08  00------  SendSequenceNumber  : 0

    --001000  MESSAGE TYPE        : CALL CONFIRMED

04  00000100  INFORMATION ELEMENT : Bearer capability
06  00000110  length              : 6
60  0-------  Extension           : 0

    -11-----  Radio Channel Req.  : dual rate support MS/full rate preferred
    ---0----  Coding Standard     : GSM standard coding
    ----0---  Transfer Mode       : Circuit Mode
    -----000  Info Transfer Cap.  : speech
04  0-------  Extension           : 0
    -0------  Coding              : octet used for extension of inf. transf. capab.
    --00----  Spare               : 00
    ----0100  speech Vers. indic. : GSM full rate speech version 3
02  0-------  Extension           : 0
    -0------  Coding              : octet used for extension of inf. transf. capab.
    --00----  Spare               : 00
    ----0010  speech Vers. indic. : GSM full rate speech version 2
00  0-------  Extension           : 0
    -0------  Coding              : octet used for extension of inf. transf. capab.
    --00----  Spare               : 00
    ----0000  speech Vers. indic. : GSM full rate speech version 1
05  -0------  Compression         : data compression not possible
    --00----  Structure           : service data unit integrity
    ----0---  Duplex Mode         : half duplex
    ------0-  Negot. of Int.      : No meaning is associated with this value.
81  1-------  Extension           : 1
    -00-----  Access ID           : octet identifier
    ---00---  Rate Adaptation     : no rate adaption
    -----001  Signalling Acc.Prot : I.440/450
```

Tafel 55: Die Meldung CALL CONFIRMED im MTC wenn die Datenübertragung nicht beauftragt ist

10.3.2 Datenübertragung im GSM ist beauftrag

Ein Leser der Datenübertragung für sein Mobile beauftragt hat, kann das wie folgt nachweisen.
Mit einem Datenkabel ist das Mobile mit einem COM-Port verbunden.. Das Hyperterminal aus dem Windows-Zubehör wird über diesen COM-Port mit dem Mobile verbunden. Jetzt kann man mit dem Mobile mittels AT-Befehlen kommunizieren. Die Verbindung zum Mobile ist funktionstüchtig, wenn man in das Hyperterminal-Fenster das Kommando „AT“ eingibt und als Antwort OK erhält. Wird nun mit FRITZ!data das Mobile angerufen, sieht man ein „RING“ im Hyperterm Fenster und wenn als Antword „ATA“ eingeben wird ein „Connect“.

10.3.3 Datenübertragung ins Internet.

Eine Verbindung ins Internet kann aufgebaut werden auch wenn Datenübertragung im GSM nicht beauftragt ist. Damit verdient der Operator nämlich Geld☺

```
_____[ 10 ]___[ 29780 ]___[ UP ]___[ NAS ]_____________

03 45 04 07  a2 88 81 21  15 63 a6 5e  05 81 10 19  10 f1

03  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0011  Protocol Discrim.   : Call control and call related SS messages
45  01------  SendSequenceNumber  : 1

    --000101  MESSAGE TYPE        : SETUP

04  00000100  INFORMATION ELEMENT : Bearer capability
07  00000111  length              : 7
a2  1-------  Extension           : 1
    -01-----  Radio Channel Req.  : full rate support only MS
    ---0----  Coding Standard     : GSM standard coding
    ----0---  Transfer Mode       : Circuit Mode
    -----010  Info Transfer Cap.  : 3.1 kHz audio, ex PLMN
88  1-------  Extension           : 1
    -0------  Compression         : data compression not possible
    --00----  Structure           : service data unit integrity
    ----1---  Duplex Mode         : full duplex
    -----0--  Configuration       : point-to-point
    ------0-  Negot. of Int.      : No meaning is associated with this value.
    -------0  Establishment       : demand
81  1-------  Extension           : 1
    -00-----  Access ID           : octet identifier
    ---00---  Rate Adaptation     : no rate adaption
    -----001  Signalling Acc.Prot : I.440/450
21  0-------  Extension           : 0
    -01-----  Layer 1 ID
    ---0000-  User Info L1 Prot   : Default layer1 protocol
    -------1  Sync/async          : asynchronous
15  0-------  Extension           : 0
    -0------  Numb Stop Bits      : 1 bit (also used in the case of synchr mode)
    --0-----  Negotiation         : in-band negotiation not possible
    ---1----  Numb Data Bits      : 8 bits (also used i case of bit oriented protocols)
    ----0101  User Rate           : 9.6 kbit/sRecommendation X.1 and V.110
63  0-------  Extension           : 0
    -11-----  Intermediate Rate   : 16 kbit/s
    ---0----  NIC On Tx           : not require to send data with network  indep.clock
    ----0---  NIC On Rx           : can't accept data with network indep. clock
    -----011  Parity              : none
a6  1-------  Extension           : 1
    -01-----  Connect Element     : non transparent (RLP)
    ---00110  Modem Type          : V.32
5e  01011110  INFORMATION ELEMENT : CalledPartyBCDNumber
05  00000101  length              : 5
81  1-------  Extension           : 1
    -000----  Type of number      : unknown
    ----0001  Numb. plan id.      : ISDN/teleph. numb. plan (Rec. E.164/E.163) _
10..f1        number              : 0191011
```

Tafel 56: SETUP einer Datenverbindung ins Internet

Eine solche Verbindung funktioniert wie ein t-online-Aufruf über ein Analog Modem oder das ISDN. Das Netz übergibt eine IP-Nummer, jedoch beträgt die Datenrate nur 9,6 Kilobit/sec.

Mit einem normalen GSM-Mobile kann über die Verbindung mit dem PC ebenfalls eine derartige Internetverbindung aufgebaut werden. Über das Icon in der Fußleiste können die Eigenschaften der Verbindung, d.h. die Übertragungsgeschwindigkeit abgelesen werden. Mit dem Kommando „ipconfig“ in einem „cmd Fenster“ kann man die zugeteilte IP-Nummer erfragen.

11. Dienstmerkmale im GSM

Im ISDN (DSS-1) wurden Dienstmerkmale auf vier verschiedene Arten realisiert

1. Die Dienstmerkmale *Direct Dialing In* (Durchwahl in Vermittlungen) und *Multi Subscriber Number* (Mehrfach Rufnummer) wurden hardwaretechnisch realisiert, das entfällt im GSM.
2. Die durch die Meldungen HOLD und RETRIEVE realisierten Dienstmerkmale im ISDN sind Call Waiting (CW) „Anklopfen“ und HOLD (Halten einer Verbindung zum Zwecke des Makelns). Diese Dienstmerkmale werden auch im GSM eingesetzt, während die Meldungen SUSPEND und RESUME, im ISDN für das „Umstecken am Bus“ (TP) eingesetzt, im GSM nicht benötigt werden.
3. Über Informationselemente wurden im ISDN die nachstehenden DM aufgerufen:

- CLIP, Calling Line Identification Presentation
  Übermittlung der Rufnummer des rufenden Tln. zum gerufenen Tln.
- CLIR, Calling Line Identification Restriction
  Unterdrückung der Übermittlung der Rufnummer des rufenden Tln.
  Im GSM werden CLIR und CLIP über ein Informationselement im SETUP des MOC geschaltet. Das funktioniert so: Ist das IE CLIR im SETUP des MOC enthalten, wird die Mobile-Nummer nicht dargestellt, ist das IE nicht enthalten gilt CLIP (die Nummer wird beim B-Teilnehmer dargestellt).
- COLP, Connected Line Identification Presentation
  Übermittlung der Rufnummer des gerufenen Tln. zum rufenden Tln.
- COLR, Connected Line Identification Restriction
  Unterdrückung der Rufnummer des gerufenen Tln. Im GSM werden COLP und COLR z.Zt. weder vom Operator D1 noch vom Operator D2 unterstützt, obwohl in der Meldung CONNECT im MTC sowohl die *Connected number* als auch *Connected subaddress* enthalten sein können. Im MOC ist ohnehin nur die *Connected subaddress* zur Übertragung vorgesehen..
- no screening Nichtüberprüfen der gesendeten Nummer durch das Netz,
  Im GSM entfällt das DM „no screening“, da die Mobile-Nummer sowieso vom Netz eingesetzt wird.
- SUB, Subaddressing
  das Versenden einer Subadresse von max. 20 Ziffern zusätzlich zur Adresse.
  Im Mobilfunk kann eine Subadresse über das dafür vorgesehen IE im SETUP des MTC und des MOC ausgetauscht werden. Im MOC ist nur die *Connected subaddress* zur Übertragung vorgesehen..

4. Die im ISDN über das IE *Facility* aufgerufenen, in der *Abstracten Syntax Notation 1* (ASN.1) codierten Dienstmerkmale existierten im GSM (modifiziert) ebenfalls. Dazu unterscheidet man im GSM (im Gegensatz zum DSS-1, aber ähnlich dem 1TR6) rufabhängige Supplementary Services (Protokoll Discriminator 3) und rufunabhängige Supplementary Services (Protokoll Discriminator B).

Diese Aussagagen sollen durch einige Übungen verifiziert werden.

11.1 Die Dienstmerkmale CLIP und CLIR

Das Dienstmerkmal CLIP ist solange wirksam, wie im MOC das IE *CLIR invocation* (A2) nicht enthalten ist.

Wie das Dienstmermal in Ihrem Mobile heißt müssen Sie herausfinden (bei SAGEM heißt es *Anonymous mode*)Wenn Sie mit Ihrem Mobile FRITZ!fon anrufen , brauchen Sie den ankommenden Ruf gar nicht anzunehmen, da Ihnen das Programm sagt, ob eine Nummer mitgeschickt wird oder nicht.

```
_____[ 12 ]___[ 1215033 ]___[ UP ]___[ NAS ]_____________

03 85 04 06  60 04 02 00  05 81 5e 07  81 10 37 26  33 01 f6 a2


03  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0011  Protocol Discrim.   : Call control and call related SS messages
85  10------  SendSequenceNumber  : 0

    --000101  MESSAGE TYPE        : SETUP

04  00000100  INFORMATION ELEMENT : Bearer capability
06  00000110  length              : 6
60  0-------  Extension           : 0

    -11-----  Radio Channel Req.  : dual rate support MS/full rate preferred
    ---0----  Coding Standard     : GSM standard coding
    ----0---  Transfer Mode       : Circuit Mode
    -----000  Info Transfer Cap.  : speech
04  0-------  Extension           : 0
    -0------  Coding              : octet used for extension of inf. transf. capab.
    --00----  Spare               : 00
    ----0100  speech Vers. indic. : GSM full rate speech version 3
02  0-------  Extension           : 0
    -0------  Coding              : octet used for extension of inf. transf. capab.
    --00----  Spare               : 00
    ----0010  speech Vers. indic. : GSM full rate speech version 2
00  0-------  Extension           : 0
    -0------  Coding              : octet used for extension of inf. transf. capab.
    --00----  Spare               : 00
    ----0000  speech Vers. indic. : GSM full rate speech version 1
05  -0------  Compression         : data compression not possible
    --00----  Structure           : service data unit integrity
    ----0---  Duplex Mode         : half duplex
    ------0-  Negot. of Int.      : No meaning is associated with this value.
81  1-------  Extension           : 1
    -00-----  Access ID           : octet identifier
    ---00---  Rate Adaptation     : no rate adaption
    -----001  Signalling Acc.Prot : I.440/450

5e  01011110  INFORMATION ELEMENT : CalledPartyBCDNumber
07  00000111  length              : 7
81  1-------  Extension           : 1
    -000----  Type of number      : unknown
    ----0001  Numb. plan id.      : ISDN/teleph. numb. plan (Rec. E.164/E.163) _
10..f6        number              : 01736233106

a2  10100010  Information Element : CLIR Invocation
```

Tafel 57: SETUP eines MOC im Anonymous mode

In Tafel 57 ist das IE *CLIR Invocation* enthalten, also wir die Telefonnumer beim Partner nicht dargestellt.

.

11.2 Das Dienstmerkmal HOLD

Aus dem ISDN wurde ein OT 460 angerufen. Nach Annahme des Rufs steht im Menü Options der Eintrag *HOLD call* zur Verfügung. Wird diese Taste gedrückt, wird das Gespräch im ISDN gehalten und dort die Ansage „Please hold the line ...“ abgespielt. Im Menü Option steht nun der Eintrag *Take back a call* zur Verfügung. Auswahl dieses Menüpunktes schaltet das Gespräch zum ISDN-Teilnehmer zurück. Tafel 58 zeigt den dazugehörenden Trace. Wie man an den Zeitmarken sehen kann, sind die Meldungen aufsteigend angeordnet. Das rührt daher, dass EDGEView das *Message log* auswertet und das wird bottom up geschrieben.

Mit einem handelsübliche Mobile kann das nachvollzogen werden, indem man Capidog startet und mit FRITZ!fon das Mobile anruft. Am Mobile wird nun ebenfalls *HOLD call* und dann *Take back a call* gedrückt (wie das bei Ihrem Mobile heißt müssen Sie herausfinden) . Sie können nun den von Capidog aufgezeichneten Trace ansehen. Sie finden den Eintrag NOTIFICATION F9 (Remote hold) und NOTIFICATION FA (Remote retrieval), wodurch das Geschehen aus der ISDN-Sicht beschrieben wird.

```
_____[ 4 ]___[ 1452205 ]___[ DOWN ]___[ NAS ]_____________

13 1d

13  0-------  direction from      : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
1d  00------  SendSequenceNumber  : 0
    --011101  MESSAGE TYPE        : RETRIEVE ACKNOWLEDGE

_____[ 5 ]___[ 1452134 ]___[ UP ]___[ NAS ]_____________

93 9c

93  1-------  direction to        : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
9c  10------  SendSequenceNumber  : 0
    --011100  MESSAGE TYPE        : RETRIEVE

_____[ 6 ]___[ 1449505 ]___[ DOWN ]___[ NAS ]_____________

13 19

13  0-------  direction from      : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
19  00------  SendSequenceNumber  : 0
    --011001  MESSAGE TYPE        : HOLD ACKNOWLEDGE

_____[ 7 ]___[ 1449352 ]___[ UP ]___[ NAS ]_____________

93 58

93  1-------  direction to        : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
58  01------  SendSequenceNumber  : 1
    --011000  MESSAGE TYPE        : HOLD
```

Tafel 58: Die Meldungen HOLD und RETRIEVE in einem MTC

11.3 ASN.1 codierte Dienstmerkmale

Dem mit ASN.1 nicht vertrauten Leser wird empfohlen den entsprechenden Abschnitt in dem auf dieser Web-Seite enthaltenen Lehrbrief „Der ISDN-D-Kanal“ zu lesen. Die dort enthaltenen Ausführungen über die Kodierung in ASN.1 werden hier nicht wiederholt.
Es muss auf einen Unterschied zum DSS-1 Verwiesen werden. Im DSS-1 war es gleichgültig ob das Dienstmerkmal während eines bestehenden Rufs aktiviert wurde (z.B. die Dreierkonferenz. (3PTY)) oder unabhängig vom Ruf (z.B. eine Rufumleitung). Im Gegensatz dazu gab es im nationalen ISDN 1TR6 die Unterscheidung zwischen rufabhängigen und rufunabhängigen Dienstmerkmalen.
Genauso ist es wieder im GSM, auch hier wird zwischen rufabhängigen und rufunabhängigen Dienstmerkmalen unterschieden. Dabei werden die rufabhängigen Dienstmerkmale über die Meldung FACILITY aufgerufen , die zu den Call Control Messages (PD 3) gehört. Die rufunabhängigen Dienstmerkmale werden über die Meldung FACILITY REGISTER augerunfen (PD B).
Zum Verständnis der in nachstehender Liste genannten Operationen muss noch erwähnt werden, dass es im ISDN eine Dreiekonferenz (3PTY) und eine Zehnerkonferenz (CONF) gibt. Im GSM gibt es eine Mischung zwischen beiden, die MultiPTY (frei übersetzt) vielfach Konferenz, mit der bis zu 6 Teilnehmer verbunden werden können..

Rufabhängige Dienstmerkmale sind:

callDeflection	Anrufweiterschaltung in der Rufphase
userUserService	Textübertragung zwischen Teilnehmern
forwardCUG-Info	Umleitung einer Information über geschlossene Benutzergruppe
buildMPTY	Herstellen einer Konferenz
splitMPTY	Herauslösen eines Teilnehmers aus der Konferenz.
holdMPTY	Halten der Konferenz
retrieveMPTY	Aktivieren einer Konferenz aus dem HOLD
forwardChargeAdvice	Umleitung einer Gebühreninformation
explicitCT	Explicit Calltransfer (Umlegen)

Rufunabhängige Dienstmerkmale sind:

Call Forwarding Unconditional,	Rufumleitung unbedingt,
Call Forwarding on Mobile Subscriber Busy,	Rufumleitung wenn der Nutzer besetzt ist,
Call Forwarding on No Reply,	Rufumleitung wenn der Nutzer nicht antwortet.
Call Waiting,	Anklopfen

GSM typisch sind:

Call Forwarding on Mobile Subscriber, Not Reachable	Rufumleitung wenn der Nutzer nicht erreichbar ist
Calling Name Presentation - $(CNAP)$,	Darstellung des Namens des Anrufers

Auf das GSM zugeschnitten ist auch die Art der Sperren:

Barring of All Outgoing Calls,	Sperre aller Ausgehenden Rufe
Barring of Outgoing International Calls,	Sperre aller ankommenden Rufe
Barring of Outgoing International Calls- except those directed to the Home PLMN- Country ,	Sperre Ausgehender Rufe, außer solcher zum - Heimat PLMN
Barring of All Incoming Calls,	Sperre aller eingehenden Rufe
Barring of Incoming Calls when Roaming- Outside the Home PLMN Country	Sperre aller eingehenden Rufe bei m Roaming- außerhalb des Heimat PLMN

Es sollte nicht vergessen werden , dass mit FACILITY REGISTER auch nach der Existenz eines DM (interogateSS), gefragt wird. Somit bedient diese Meldung praktisch alle Dienstmerkmale. Das kann aus der Liste der ss-codes in Tafel 55 abgelesen werden.

11.3.1 Rufabhängige Dienstmerkmale

Ein sehr einfache ASN.1 Konstruktion stellt die Kodierung des Dienstmerkmals **M**ulti**P**ar**TY** dar. Im ISDN bekannt als Dreierkonferenz bzw Coference call add one. Mit dem OT 460 wurde eine Konferenz vom Typ MTPY gestartet mit der 3 bis 6 Teilnehmer miteinander verbunden werden können. Der Mechanismus besteht darin, zunächst mit einem Partner Verbindung aufzunehmen, diesen dann zu halten, den dritten Teilnehmer anzurufen und dann alle drei mit dem Aufruf „collect calls“,den man im Menü Optionen findet, auf den Konferenzblock im Netz zu legen.
Die Leitung der Konferenz behält der Aufrufende, der die Konferenz ja auch bezahlt.

Sie können mit Ihrem eigenen Mobile die Übung selbständig auf eine Verbindung mit bis zu 6 Teilnehmern erweitern. Mit Capidog können Sie den (1.) Teilnehmer FRITZ!fon tracen. Was in derKonferenz geschieht wird Ihnen mit
NOTIFICATION FA
NOTIFICATION XX
mitgeteilt, wobei XX die nachstehenden Werte mit der entsprechende Bedeutung annehmen kann.

80 user suspended
81 user resumed
82 beare service changed
84 Call completion delay
83 Discriminator for Extension to ASN.1 encoded component
C2 Conference established
C3 Conference disconnected
C4 Other Party added
CA Isolated
C6 Reattached
C7 Other party isolated
C8 Other party reattached
C9 Other party splitt
CA Other party disconnected
CB Conference floating
CF Conference floating, served user preemted
CC Conference disconnected,preemtion
F9 Remote hold
FA Remote retrieval
E0 Call is a waiting call
EB Call is diverting
E8 Diversion activated

Im Traceausschnitt (Tafel 59) wird die Aktivierung des DM *buildMPTY* in der Meldung FACILITY aufgerufen.
Sie erkennen die typische ASN.1 Schreibweise. D.h. mit der Meldung FACILITY wird stets eine Komponente aufgerufen. Diese Komponente heißt hier Invoke:

.

```
_____[ 11 ]___[ 2560992 ]___[ UP ]___[ NAS ]_____________

93 7a 08 a1  06 02 01 02  02 01 7c 7f  01 00

93  1-------  direction to        : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
7a  01------  SendSequenceNumber  : 1
```

```
    --111010  MESSAGE TYPE        : FACILITY
08  00001000  Lgth OF IE FACILITY : 8
a1  10100001  Component            : Invoke
06  00000110  length               : 6

02  00000010  Type=INTEGER         : Invoke Identifier
01  00000001  length               : 1
02  00000010  Inv.ID. Value        : 2

02  00000010  Type=INTEGER         : Operation Value
01  00000001  length               : 1
7c  01111100  Operation Value      : buildMPTY


7f  01111111  Information Element : SS-Version
01  00000001  length              : 1
00  00000000  SS-Version indicator: 0
```

Tafel 59: Inhalt der Meldung MTPY

Im Lehrbrief über den ISDN-D-Kanal wurde ausführlich erklärt, dass eine Komponente aus einem Typ, einer Länge und einem Wert (Format TLV) besteht. Im Beispiel stellt die Komponente *Invoke* einen zusammengesetzten Typ dar, d.h. der Wert (V) von *Invoke* besteht aus zwei einfachen (primitiven) Typen, dem Aufrufbezeichner und dem Operationswert. Außer der Komponente

(a1) *Invoke* = Aufruf,

gibt es noch die Komponenten

(a2) *ReturnResult* = Zurückgegebenes Ergebnis (durch das Netz),
(a3) *Error* = Fehler,
(a4) *Reject* = Zurückweisung.

Nachstehend sind alle Komponenten die die Meldung FACILITY im PD3 transportieren kann aufgeführt. Der in jeder Komponente enthaltene *Invoke Identifier* (Aufrufbezeichner) ist eine Integerzahl die den Aufruf eindeutig kennzeichnet.. Der *Operation Value* (Operationswert) ist ebenfalls eine ganze Zahl deren Bedeutung der in Tafel 52 dargestellten Liste entnommen wird. Das ist dem DSS-1 sehr ähnlich.

```
00010000  Operation Value    : NotifySS
01110101  Operation Value    : callDeflection
01110110  Operation Value    : userUserService
01110111  Operation Value    : accessRegisterCCEntry
01111000  Operation Value    : forwardCUG-Info
01111001  Operation Value    : splitMPTY
01111010  Operation Value    : retrieveMPTY
01111011  Operation Value    : holdMPTY
01111100  Operation Value    : buildMPTY
01111101  Operation Value    : forwardChargeAdvice
01111110  Operation Value    : explicitCT
01110100  Operation Value    : lcs-LocationNotification
01110011  Operation Value    : lcs-MOLR LCS-MOLR
```

Tafel 60: Operationwerte für Rufabhängige Dienstmerkmale (Auswahl)

DasMobile OT 460 unterstützt nicht alle die MPTY betreffenden Optionen, mit denen es möglich sein sollte Teilnehmer zeitweilig aus der Konferenz zu entlassen und wieder einzubeziehen, etc..

11.3.2 Rufunabhängige Dienstmerkmale

Ein einfaches rufabhängiges DM ist “Call waiting“ (CW), zu deutsch Anklopfen, im OT 460 „Double Call“, wird das DM im Menü *Setting -> Calls -> Call waiting* aktiviert.

Wenn Sie angerufen werden während Sie mit einem anderen Partner telefonieren, erhalten Sie im laufenden Gespräch ein Signal (Anklopfton). Sie können dann entscheiden, ob sie das Gespräck annehmen wobei der monmentane Partner gehalten wird, oder abweisen, dann erhält der Rufer das Besetztzeichen. .

Der Aufrufs eines rufunabhängigen Dienstmerkmaleserfolgt über die Meldung FACILITY REGISTER. Diese Meldung wird vom Netz mit RELEASE COMPLETE beantwortet. Beide Meldungen tragen den Prozess Discriminator „B“. Sie finden in FACILITY REGISTER (Tafel 53) ein Informationselement Facility, das wieder eine Komponente befördert. Wie in der Meldung FACILITY gibt es die vier verschiedenen Komponenten Invoke, Return Result, Error und Reject..

Die Komponente Invoke in Tafel 61 enthält den Invoke Identifier (Aufrufbezeichner) und den Operationswert. Der Operationswert wird hier aber nicht, wie bei den rufabhängigen Dienstmerkmalen durch einen Begriff, ohne weitere Erklärungen, gebildet, sondern zunächst durch die Beschreibung der Operation.
Diese Operationen können zum Beispiel sein:
Registrieren eines DM (registerSS), Löschen einer Registrierung (eraseSS), Aktivieren eines DM (activateSS), Deaktivieren eines DM (deactivateSS), Anfragen nach der Existenz eines DM (interrogateSS), Informieren eines Partners über die Existenz eines DM (notifySS).

Im Beispiel lautet die Operation *registerSS.* Nun muss dem Netz noch mitgeteilt werden was registriert werden soll. Im Trace folgt daher eine Aufzählung dessen, bezeichnet mit *registerSS-Argument.* Dabei stellt der Typ SEQUENCE eine Klammer um eine mit *length* gekennzeichnet Anzahl nachfolgender Begriffe dar.

```
_____[ 10 ]___[ 2713275 ]___[ UP ]___[ NAS ]_____________

0b bb 1c 19  a1 17 02 01  02 02 01 0a  30 0f 04 01  21 83 01 10
84 07 81 30  73 25 01 18  55 7f 01 00

0b  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----1011  Protocol Discrim.   : non call related SS messages
bb  10------  SendSequenceNumber  : 0

    --111011  MESSAGE TYPE        : FACILITY REGISTER

1c  00011100  INFORMATION ELEMENT : Facility
19  00011001  length              : 25
a1  10100001  Component           : Invoke
17  00010111  length              : 23

02  00000010  Type=INTEGER        : Invoke Identifier
01  00000001  length              : 1
02  00000010  Inv.ID. Value       : 2

02  00000010  Type=INTEGER        : Operation Value
01  00000001  length              : 1
0a  00001010  Operation Value     : registerSS

30  00110000  SEQUENCE            : registerSS-Arg
0f  00001111  lenght              : 15


04  00000100  IMPL.OCTETSTRING    : ss-code
01  00000001  length              : 1
21  00100001  ss-code Value       : cfu



83  10000011  IMPL. OCTETSTRING   : teleservice
01  00000001  length              : 1
10  00010000  Teleservice         : speech


84  10000100  INFORMATION ELEMENT : forwardedToNumber
07  00000111  length              : 7
81  1-------  Extension           : 1
    -000----  Type of number      : unknown
    ----0001  Numb. plan id.      : ISDN/teleph. numb. plan (Rec. E.164/E.163) _
30..55        number              : 033752108155
```

```
7f  01111111  INFORMATIONSELEMENT : SS Version Indicator
01  00000001  length             : 1
00  00000000  SS-Versions Info.   : 0
```

Tafel 61: Inhalt einer Meldung FACILITY REGISTER

Das Netz antwortet mit der Meldung RELEASE COMPLETE (Tafel 62), in der das Informationselement Facility die Komponente ReturnResult mit einer ausführlichen Antwort zurückgibt.

```
_____[ 7 ]___[ 2713632 ]___[ DOWN ]___[ NAS ]_____________

8b 2a 1c 23  a2 21 02 01  02 30 1c 02  01 0a a0 17  04 01 21 30
12 30 10 83  01 10 84 01  07 85 08 91  94 33 57 12  80 51 f5

8b  1-------  direction to        : originating site
    -000----  TransactionID       : 0
    ----1011  Protocol Discrim.   : non call related SS messages
2a  00------  SendSequenceNumber  : 0

    --101010  MESSAGE TYPE        : RELEASE COMPLETE

1c  00011100  INFORMATION ELEMENT : Facility
23  00100011  Lgth of IE FACILITY : 35
a2  10100010  Component           : ReturnResult
21  00100001  length              : 33

02  00000010  Type=INTEGER        : Invoke Identifier
01  00000001  length              : 1
02  00000010  Inv.ID. Value       : 2

30  00110000  SEQUENCE            : Resultinfo
1c  00011100  length              : 28
02  00000010  INTEGER             : OperationValue
01  00000001  length              : 1
0a  00001010  Operation Value     : RegisterSS

a0  10100000  IMPLICIT SEQUENCE   : Forwarding Info
17  00010111  length              : 23

04  00000100  IMPL.OCTETSTRING    : ss-code
01  00000001  length              : 1
21  00100001  ss-code Value       : cfu

30  00110000  SEQUENCE            : forwardingFeatureList
12  00010010  length              : 18
30  00110000  SEQUENCE            : basicService
10  00010000  length              : 16

83  10000011  IMPL. OCTETSTRING   : teleservice
01  00000001  length              : 1
10  00010000  Teleservice         : speech

84  10000100  OCTETSTRING         : ss-status
01  00000001  length              : 1
07  00000111  P,R und A-bit       : Active and Operative, Registered, Provisioned

85  10000101  IMPL. OCTETSTRING   : forwardedToNumber
08  00001000  length              : 8
91  1-------  Extension           : 1
    -001----  Type of number      : international number
    ----0001  Numb. plan id.      : ISDN/telephony numb. pl. (Rec. E.164/E.163)
94  1-------  Extension           : 1
    -00-----  Present.indic.      : Presentation allowed
    ------00  Screening ind.      : User-provided, not screened
33..f5        number              : 33752108155
```

Tafel 62: Inhalt einer Meldung RELEASE COMPLETE (SS)

Nachstehende Dienstmerkmale sind vom Ruf unabhängig. Neben dem in der Übung verwendeten Dienstmerkmal

CFU Call Forwarding Unconditional, Rufumleitung unbedingt,

gehören u.A. noch die aus dem ISDN bekannten dazu:

CFB Call Forwarding on Mobile Subscriber Busy, Rufumleitung wenn der Nutzer besetzt ist,
CFNRy Call Forwarding on No Reply, Rufumleitung wenn der Nutzer nicht antwortet.
CW Call Waiting, Anklopfen

GSM –typisch sind:

CFNR*c* Call Forwarding on Mobile Subscriber Not Reachable, Rufumleitung wenn der Nutzer nicht erreichbar ist
CNA*P* Calling Name Presentation - $(CNAP)$, Darstellung des Namens des Anrufers

Auf das GSM zugeschnitten ist auch die Art der Sperren:

BAOC Barring of All Outgoing Calls, Sperre aller Ausgehenden Rufe
BOIC Barring of Outgoing International Calls, Sperre aller ankommenden Rufe
BOIC-exHC Barring of Outgoing International Calls except those directed to the Home PLMN Country , Sperre Ausgehender Rufe, außer solcher zum Heimat PLMN
BAIC Barring of All Incoming Calls, Sperre aller eingehenden Rufe
BIC-Roam Barring of Incoming Calls when Roaming Outside the Home PLMN Country Sperre aller eingehenden Rufe bei m Roaming außerhalb des Heimat PLMN

Mit FACILITY REGISTER wird auch nach der Existenz eines DM (interogateSS), gefragt. Somit bedient diese Meldung praktisch alle Dienstmerkmale. Das ist aus der Liste der ss-codes in Tafel 55 ablesbar.

Es ist sicherlich von Interesse ob im GSM das DM CCBS „Rückruf bei besetzt“ existiert. Wie aus Tafel 55 hervorgeht, ist es in den Standards enthalten, aber bis jetzt ist dem Autot kein Mobile bekannt, das dieses Merkmal implementiert hat. Auch bei einem Anruf aus dem Festnetz erhält man beim Anruf eines Mobiles von dem aus gerade gesprochen wird keine Aufforderung CCBS anzumelden.

00010001 ss-code Value : clip
00010010 ss-code Value : clir
00010011 ss-code Value : colp
00010100 ss-code Value : colr
00100000 ss-code Value : allForwardingSS
00100001 ss-code Value : cfu
00101000 ss-code Value : allCondForwardingSS
00101001 ss-code Value : cfb
00101010 ss-code Value : cfnry
00101011 ss-code Value : cfnrc
00100100 ss-code Value : cd
00110001 ss-code Value : ect
01000001 ss-code Value : cw
01000011 ss-code Value : ccbs-A(origination side)
01000100 ss-code Value : ccbs-B(destination side)
01000010 ss-code Value : hold
01010001 ss-code Value : multiPTY
01110001 ss-code Value : aoci (information)
01110010 ss-code Value : aocc (charging)
10000001 ss-code Value : uus1
10000010 ss-code Value : uus2
10000011 ss-code Value : uus3
10010000 ss-code Value : allBarringSS
10010001 ss-code Value : barrinOfOutgoingCalls

10010010 ss-code Value : baoc
10010011 ss-code Value : boic
10010100 ss-code Value : boicExHC
10011001 ss-code Value : barringOfincomingCalls
10011010 ss-code Value : baic
10011011 ss-code Value : bicRoam

Tafel 63: SS-codes (Auswahl) nach GSM 09.02

.

12. Die Übertragung von SMS

Der Short Message Service (SMS) ist eine beliebte Informationsart, nicht nur jugendlicher GSM-Mobilebesitzer, der vorallem dem Austausch kurzer Textnachrichten dient.
Im Gegensatz dazu kann man mit einem GPRS-tauglichen Mobile auch MMS versenden, d.h. mit dem *Multi Media Message Service* Texte, Bilder und Töne.

Es existiert noch der Edvanced Message Service EMS der eine Zwischenstellung zwischen SMS und MMS einnimmt.

12.1 Eine SMS empfangen

Sämtliche Meldungen die in einer empfangenen, kurzen SMS auftreten sind in Bild 38 dargestellt.

55	0x03 - LAPD-m	CCCH	Down	(RR : PAGING REQUEST TYPE 1)	15 06 21 00 01 F0 8B 2B 2B 2B 2B 2B 2B 2B 2E
56	0x03 - LAPD-m	RACH	Up	RR CHANNEL REQUEST	
57	0x03 - LAPD-m	CCCH	Down	(RR : PAGING REQUEST TYPE 1)	25 06 21 20 05 F4 2E 05 7E 9A 81 2B 2B 2B 2B 2B
58	0x03 - LAPD-m	CCCH	Down	(RR : PAGING REQUEST TYPE 1)	15 06 21 00 01 F0 8B 2B 2B 2B 2B 2B 2B 2B 2E
59	0x03 - LAPD-m	CCCH	Down	(RR : PAGING REQUEST TYPE 1)	15 06 21 00 01 F0 8B 2B 2B 2B 2B 2B 2B 2B 2E
60	0x03 - LAPD-m	CCCH	Down	(RR : IMMEDIATE ASSIGNMENT)	2D 06 3F 00 4A 60 04 23 2A 01 01 00 2B 2B 2B 2B
61	0x00 - RadioRessource		Up	RR : PAGING RESPONSE	06 27 05 03 53 19 81 05 F4 2E 05 45 96
62	0x03 - LAPD-m	SDCCH	Up	SABM (RR : PAGING RESPONSE)	01 3F 35 06 27 05 03 53 19 81 05 F4 2E 05 45 96
63	0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 5)	03 03 49 06 1D 10 00 00 00 00 00 81 11 41 04 00 00
64	0x00 - RadioRessource		Down	RR : SYSTEM INFORMATION TYPE 5	06 1D 10 00 00 00 00 00 81 11 41 04 00 00 00 00 02
65	0x03 - LAPD-m	SDCCH	Down	UA (RR : PAGING RESPONSE)	01 73 35 06 27 05 03 53 19 81 05 F4 2E 05 45 96
66	0x00 - RadioRessource		Up	RR : CLASSMARK_CHANGE	06 16 03 53 19 81 20 08 60 14 54 76 15 7B 00 00
67	0x03 - LAPD-m	SDCCH	Up	I (RR : CLASSMARK_CHANGE)	01 00 41 06 16 03 53 19 81 20 08 60 14 54 76 15 7E
68	0x03 - LAPD-m	SDCCH	Down	I (MM : AUTHENTIFICATION REQUEST)-L3 SEG BEGIN	03 20 53 05 12 06 A3 52 8B A5 0E 67 DB 68 08 36 2
69	0x03 - LAPD-m	SDCCH	Up	RR	03 21 01
70	0x00 - RadioRessource		Up	RR : MEASUREMENT REPORT	06 15 00 40 00 00 00 00 00 00 00 00 00 00 00 00
71	0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 00 40 00 00 00 00 00 00 00 00 00
72	0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 5ter)	03 03 49 06 06 DF 6A A8 00 00 00 00 00 00 00 00 0
73	0x00 - RadioRessource		Down	RR : SYSTEM INFORMATION TYPE 5ter	06 06 DF 6A A8 00 00 00 00 00 00 00 00 00 00 00 0
74	0x02 - NAS		Down	MM : AUTHENTIFICATION REQUEST	05 12 06 A3 52 8B A5 0E 67 DB 68 08 36 2A 6C 22
75	0x03 - LAPD-m	SDCCH	Up	RR	03 41 01
76	0x02 - NAS		Up	MM : AUTHENTIFICATION RESPONSE	05 14 05 CD A1 C1
77	0x03 - LAPD-m	SDCCH	Up	I (MM : AUTHENTIFICATION RESPONSE)	01 42 19 05 14 05 CD A1 C1
78	0x00 - RadioRessource		Up	RR : MEASUREMENT REPORT	06 15 00 40 00 00 00 00 00 00 00 00 00 00 00 00
79	0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 00 40 00 00 00 00 00 00 00 00 00
80	0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 6)	03 03 2D 06 1E 06 38 62 F2 20 01 3C 95 F8 7B 2B 2
81	0x00 - RadioRessource		Down	RR : SYSTEM INFORMATION TYPE 6	06 1E 06 38 62 F2 20 01 3C 95 F8 7B 2B 2B 2B 2B
82	0x00 - RadioRessource		Down	RR : CIPHERING MODE COMMAND	06 35 01
83	0x00 - RadioRessource		Down	RR : CIPHERING MODE COMMAND	06 35 01
84	0x03 - LAPD-m	SDCCH	Up	RR	03 61 01
85	0x00 - RadioRessource		Up	RR : CIPHERING MODE COMPLETE	06 32
86	0x03 - LAPD-m	SDCCH	Up	I (RR : CIPHERING MODE COMPLETE)	01 64 09 06 32
87	0x00 - RadioRessource		Up	RR : MEASUREMENT REPORT	06 15 92 12 01 11 05 6B 1D E4 47 6A 29 68 00 00 0
88	0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 92 12 01 11 05 6B 1D E4 47 6A 29 6
89	0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 5)	03 03 49 06 1D 10 00 00 00 00 00 81 11 41 04 00 00
90	0x00 - RadioRessource		Down	RR : SYSTEM INFORMATION TYPE 5	06 1D 10 00 00 00 00 00 81 11 41 04 00 00 00 00 02
91	0x03 - LAPD-m	SDCCH	Down	I (MM : TMSI REALLOCATION COMMAND)	03 66 35 05 1A 62 F2 20 01 3C 05 F4 2E 05 8C A2 2
92	0x02 - NAS		Down	MM : TMSI REALLOCATION COMMAND	05 1A 62 F2 20 01 3C 05 F4 2E 05 8C A2
93	0x03 - LAPD-m	SDCCH	Up	RR	03 81 01
94	0x02 - NAS		Up	MM : TMSI REALLOCATION COMPLETE	05 5B
95	0x03 - LAPD-m	SDCCH	Down	SABM	0F 3F 01
96	0x03 - LAPD-m	SDCCH	Up	UA	0F 73 01
97	0x00 - RadioRessource		Up	RR : MEASUREMENT REPORT	06 15 94 14 01 16 3B CA 02 B4 D2 D1 E3 B4 00 00
98	0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 94 14 01 16 3B CA 02 B4 D2 D1 E3
99	0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 5ter)	03 03 49 06 06 DF 6A A8 00 00 00 00 00 00 00 00 0
100	0x00 - RadioRessource		Down	RR : SYSTEM INFORMATION TYPE 5ter	06 06 DF 6A A8 00 00 00 00 00 00 00 00 00 00 00 0
101	0x03 - LAPD-m	SDCCH	Down	I (SMS : CP DATA)	0F 00 53 19 01 25 01 00 07 91 94 71 22 72 30 33 00
102	0x03 - LAPD-m	SDCCH	Up	I (MM : TMSI REALLOCATION COMPLETE)	01 86 09 05 5B
103	0x03 - LAPD-m	SDCCH	Down	RR	01 81 01
104	0x00 - RadioRessource		Up	RR : MEASUREMENT REPORT	06 15 93 13 01 16 3B CA 02 B5 12 D1 E3 B4 00 00
105	0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 93 13 01 16 3B CA 02 B5 12 D1 E3
106	0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 6)	03 03 2D 06 1E 06 38 62 F2 20 01 3C 95 F8 7B 2B 2
107	0x00 - RadioRessource		Down	RR : SYSTEM INFORMATION TYPE 6	06 1E 06 38 62 F2 20 01 3C 95 F8 7B 2B 2B 2B 2B
108	0x03 - LAPD-m	SDCCH	Down	I (SMS : CP DATA)	0F 10 53 19 01 25 01 00 07 91 94 71 22 72 30 33 00
109	0x03 - LAPD-m	SDCCH	Up	REJ	0F 39 01
110	0x03 - LAPD-m	SDCCH	Down	I (CC : STOP DTMF ACKNOWLEDGE)	0F 02 51 63 32 13 60 00 00 60 11 20 51 51 91 40 06
111	0x02 - NAS		Down	SMS : CP DATA	19 01 25 01 00 07 91 94 71 22 72 30 33 00 19 04 0C
112	0x03 - LAPD-m	SDCCH	Up	RR	0F 41 01
113	0x00 - RadioRessource		Up	RR : MEASUREMENT REPORT	06 15 92 12 01 15 3B C9 02 B4 52 D2 03 B4 00 00 0
114	0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 92 12 01 15 3B C9 02 B4 52 D2 03 B
115	0x02 - NAS		Up	SMS : CP ACK	99 04
116	0x02 - NAS		Up	SMS : CP DATA	99 01 02 02 00
117	0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 5)	03 03 49 06 1D 10 00 00 00 00 00 81 11 41 04 00 00
118	0x00 - RadioRessource		Down	RR : SYSTEM INFORMATION TYPE 5	06 1D 10 00 00 00 00 00 81 11 41 04 00 00 00 00 02
119	0x00 - RadioRessource		Up	RR : MEASUREMENT REPORT	06 15 93 13 01 14 3B C9 82 B4 C7 6A 29 68 00 00 0
120	0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 93 13 01 14 3B C9 82 B4 C7 6A 29 6

Bild 38: Trace des Empfangs einer kurzen SMS

Einem Paging Request auf die TMSI des Mobiles folgt der CHANNEL REQUEST in Zeile 56, den das Netz wie üblich mit IMMEDIATE ASSIGNMENT beantwortet und Arbeitsfrequenz und Zeitschlitz zuordnet (Zeilen 60). Es folgt das PAGING RESPONSE des Mobiles mit Anforderung des Protected Mode. CLASSMARK CHANGE meldet die Eigenschaften des Mobiles. AUTHENTICATION REQUEST ist hier länger als 23 Oktett und muss daher segmentiert werden. Nach AUTEHENTICATION RESPONSE folgt der Befehl zur Verschlüsselung. Nach CIPHERING MODE COMPLETE folgt das für die SMS Communication typische TMSI REALLOCATION

COMMAND (Zeile 92) und nach Bestätigung desselben in Zeile 94 fordert nun das Netz mit SABME erneut den Übergang zu acknowledged Mode an.
Es folgen nun in Zeile 101 und 108 zwei Meldungen CP DATA, die (segmentiert) die SMS enthalten.
In Zeile 111 ist die SMS als NAS –Message zusammengesetzt enthalten. Betrachten Sie dazu Bild 34.

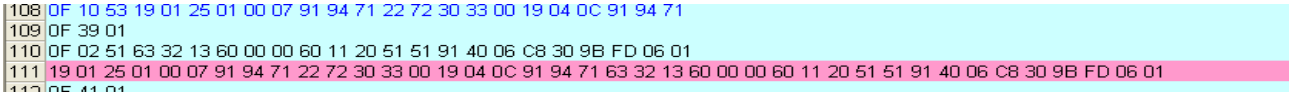


Bild 39: NAS Message einer kurzen SMS

In den Zeilen 115 und 116 folgen dann nur noch Quittungen. Tafel 56 zeigt die Übersetzung des in Bild 34 dargestellten Strings.
Die SMS wird über das SMS Control-Center (blau) zur Zieladresse (grün) geschickt. Von Bedeutung ist die Kodierung der Nachricht (rot). Eine SMS darf 160 Zeichen lang sein .Aus Platzersparnis werden nur 7 bit pro Zeichen aufgewendet, damit brauchen nur 160x7/8=140 Byte über den Kanal gesendet werden.
Die Kodierung erfolgt wie nachstehend demonstriert:

```
       : User Data
       04  00000100  lgth of 7 bit char : 4
       f4  11110100  t
       f2  11110010  e
       9c  10011100  s
       0e  00001110  t
```

Der SAPI ist bei SMS stets 3.

```
_____[ 4 ]___[ 312276 ]___[ DOWN ]___[ NAS ]_____________

19 01 25 01  00 07 91 94  71 22 72 30  33 00 19 04  0c 91 94 71
63 32 13 60  00 00 60 11  20 51 51 91  40 06 c8 30  9b fd 06 01


19  0-------  direction from      : originating site
    -001----  TransactionID       : 1
    ----1001  Protocol Discrim.   : SMS messages


01  00000001  MESSAGE TYPE        : CP DATA

: Length of SMS
25  00100101  lenght              : 37
: Parameter
01  00000001  Parameter           : 1
00  00000000  Parameter           : 0

: SMSC Address
07  00000111  lenght              : 7

91  1-------  Extension
    -001----  Type of number      : International number
    ----0001  Numbering plan      : ISDN/telephone numberingplan(E.164/E.163)
94..33        number              : 491722270333

: Message Flags
00  00000000  TP-MTI, TP-MMS, TP-SRI, TP-UDIH, TP-RP

: Message Reference Number
19  00011001  Reference Number    : 25

04  00000100  Parameter

: Destination address

0c  00001100  length              : 12
91  1-------  Extension           : 1
```

```
    -001----  Type of number      : international number
    ----0001  Numb. plan id.      : ISDN/telephony numb. pl. (Rec. E.164/E.163)
94..60        number              : 491736233106

: Protocol Identifier
00  00000000  Protocol Identifier
: Data Coding Sheme
00  00000000  Data Coding Sheme
: Parameter
60  01100000  Parameter1
11  00010001  Parameter2
20  00100000  Parameter3
51  01010001  Parameter4
51  01010001  Parameter5
91  10010001  Parameter6
40  01000000  Parameter7

: User Data
06  00000110  SMS_LENGTH          : 6
              SMS_TEXT            : Hallo
```

Tafel 64: Empfang einer kurzen SMS

.

12.2 Eine normal SMS senden

Der Beginn des Traces ist in Bild 40 dargestellt

22	0x03 - LAPD-m	BCCH	Down	(RR : IMMEDIATE ASSIGNMENT)	2D 06 3F 03 52 40 5A EB 88 2C 03 00 2B 2B
23	0x02 - NAS		Up	MM : CM SERVICE REQUEST	05 24 14 03 33 19 81 05 F4 04 CB BB B2
24	0x03 - LAPD-m	SDCCH	Up	SABM (MM : CM SERVICE REQUEST)	01 3F 35 05 24 14 03 33 19 81 05 F4 04 CB E
25	0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 6)-L3 SEG BEGIN	03 03 2D 06 1E DB D9 62 F2 10 36 0C 55 08
26	0x00 - RadioRessource		Down	RR : SYSTEM INFORMATION TYPE 6	06 1E DB D9 62 F2 10 36 0C 55 08 2B 2B 2E
27	0x00 - RadioRessource		Up	RR : CLASSMARK_CHANGE	06 16 03 33 19 81 20 08 60 14 54 76 15 7B 0
28	0x00 - RadioRessource		Up	RR : CLASSMARK_CHANGE	06 16 03 33 19 81 20 08 60 14 54 76 15 7B 0
29	0x03 - LAPD-m	SDCCH	Up	I (RR : CLASSMARK_CHANGE)	01 00 41 06 16 03 33 19 81 20 08 60 14 54 7
30	0x00 - RadioRessource		Up	RR : MEASUREMENT REPORT	06 15 00 40 00 00 00 00 00 00 00 00 00 00
31	0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 00 40 00 00 00 00 00 00 00 0
32	0x03 - LAPD-m	SDCCH	Down	I (RR : CLASSMARK ENQUIRY)	03 20 09 06 13 2B 2B 2B 2B 2B 2B 2B 2B 2E
33	0x00 - RadioRessource		Down	RR : CLASSMARK ENQUIRY	06 13
34	0x03 - LAPD-m	SDCCH	Up	RR	03 21 01
35	0x00 - RadioRessource		Up	RR : CLASSMARK_CHANGE	06 16 03 33 19 81 20 08 60 14 54 76 15 7B 0
36	0x00 - RadioRessource		Down	RR : SYSTEM INFORMATION TYPE 5	06 1D 10 00 00 00 00 10 00 00 00 00 00 0A 2
37	0x03 - LAPD-m	SDCCH	Down	I (MM : AUTHENTIFICATION REQUEST)	03 22 4D 05 12 02 C9 05 96 74 AE 25 7A 81 1
38	0x02 - NAS		Down	MM : AUTHENTIFICATION REQUEST	05 12 02 C9 05 96 74 AE 25 7A 81 20 23 2D
39	0x03 - LAPD-m	SDCCH	Up	I (RR : CLASSMARK_CHANGE)	01 42 41 06 16 03 33 19 81 20 08 60 14 54 7
40	0x02 - NAS		Up	MM : AUTHENTIFICATION RESPONSE	05 54 8A 21 03 12
41	0x00 - RadioRessource		Up	RR : MEASUREMENT REPORT	06 15 00 40 00 00 00 00 00 00 00 00 00 00
42	0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 00 40 00 00 00 00 00 00 00 0
43	0x03 - LAPD-m	SDCCH	Down	RR	01 41 01
44	0x03 - LAPD-m	SDCCH	Up	I (MM : AUTHENTIFICATION RESPONSE)	01 44 19 05 54 8A 21 03 12
45	0x03 - LAPD-m	SACCH	Down	I (RR : SYSTEM INFORMATION TYPE 6)	03 03 2D 06 1E DB D9 62 F2 10 36 0C D5 08
46	0x00 - RadioRessource		Down	RR : SYSTEM INFORMATION TYPE 6	06 1E DB D9 62 F2 10 36 0C D5 08 2B 2B 2E
47	0x00 - RadioRessource		Up	RR : MEASUREMENT REPORT	06 15 00 40 00 00 00 00 00 00 00 00 00 00
48	0x03 - LAPD-m	SACCH	Up	I (RR : MEASUREMENT REPORT)	01 03 49 06 15 00 40 00 00 00 00 00 00 00 0

Bild 40: Traceausschnitt SMS senden

Der Unterschied gegenüber Bild 33 besteht darin, dass nach der Kanalanforderung (im Bild nicht dargestellt) die Meldung CM SERVICE REQUEST (Tafel 65) den *Short message service* beauftragt.

```
_____[ 9 ]___[ 3729494 ]___[ UP ]___[ NAS ]_____________

05 24 14 03  33 19 81 05  f4 04 cb bb  b2

05  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0101  Protocol Discrim.   : mobility management messages non GPRS
24  00------  SendSequenceNumber  : 0

    --100100  MESSAGE TYPE        : CM SERVICE REQUEST

14  0-------  spare               : 0
```

```
    -001----  value for the ciphering key sequence number = 1
    ----0100  Requ.service type   : Short message service

: Mobile Station Classmark 2
03  00000011  length              : 3

33  0-------  1 spare             : 0
    -01-----  Revision Level      : Used by phase 2 mobile stations
    ---1----  "Controlled Early Classmark Sending" option is implemented in the MS
    ----0---  Encryp.Algor. A5_1  : available
    -----011  RF power capability : Class 4, handheld

19  0-------  1 spare bit         : 0
    -0------  pseudo-synch.capab. : not present
    --01----  SS Screening Indic. : phase 2 error handling
    ----1---  Mobile station supports mobile terminated point to point SMS
    -----0--  no VoiceBroadcastService (VBS) capability or no notifications wanted
    ------0-  no VoiceGroupCallService (VGCS) capability or no notifications wanted
    -------1  The MS does support the E-GSM or R-GSM

81  1-------  The MS does support any options that are indicated in CM3
    -0------  1 spare bit         : 0
    --0-----  LocationServiceValueAdded Capability  not supported
    ---0----  1 spare bit         : 0
    ----0---  SoLSA Capability    : not supported
    -----0--  Network initiated MO CM connection request not supported.
    ------0-  encryp.algorith.A5/3: not available
    -------1  encryp.algorith.A5/2: available

: Mobile identity

05  00000101  length              : 5

f4  ----0---  No. of ID digits     : even
    -----100  Type of identity     : TMSI/P-TMSI
    1111----  Identity Digit 1     : 95
04  00000100  Identity Digit 2,3   : take hex value
cb  11001011  Identity Digit 4,5   : take hex value
bb  10111011  Identity Digit 6,7   : take hex value
b2  10110010  Identity Digit 8,9   : take hex value
```

Tafel 65: Die Meldung CM SERVICE REQUEST fordert den *Short message service* an

Der weiter Ablauf im Trace entspricht Bild 38. Die in Bild 39 dargestellte Meldung CP Data beim Senden der SMS entspricht weitgehend der Meldung beim Empfang Tafel 66.

```
_____[ 4 ]___[ 3730158 ]___[ UP ]___[ NAS ]_____________

39 01 2e 00  00 00 08 81  00 94 71 22  72 30 f3 21  11 a2 0b 81
10 37 26 33  01 f6 00 00  ff 15 c8 30  9b fd 06 a9  df 2c 10 39
3c 07 9d cb  68 3a 48 1d  06

39  0-------  direction from      : originating site
    -011----  TransactionID       : 3
    ----1001  Protocol Discrim.   : SMS messages


01  00000001  MESSAGE TYPE        : CP DATA

: Length of SMS
2e  00101110  lenght              : 46
: Parameter
00  00000000  Parameter           : 0
00  00000000  Parameter           : 0
00  00000000  Parameter           : 0

08  00001000  lenght              : 8

81  1-------  Extension
    -000----  Type of number      : Unknown
    ----0001  Numbering plan      : ISDN/telephone numberingplan(E.164/E.163)
00..f3        number              : 0049172227033

21  0-------  TP-Reply-Path       : parameter is not set in this SMS-SUBMIT/DELIVER
    -0------  TP-UDHI             : The TP-UD field contains only the short message
    --1-----  TP-SRR              : A status report will be returned to the SME
```

```
    ---00---  TP-VPF              : field not present
    -----0--  TP-RD               : Instruct the SC to accept an SMS-SUBMIT for an SM still
held in the SC
    ------01  TP-MTI              : SMS-SUBMIT (in the direction MS to SC)

11  ----000-  Reference Number  high part
a2  10100010  Reference Number  low part

: Destination address

0b  00001011  length              : 11
81  1-------  Extension           : 1
    -000----  Type of number      : unknown
    ----0001  Numb. plan id.      : ISDN/telephony numb. pl. (Rec. E.164/E.163)
10..f6        number              : 01736233106

00  00000000  TP-Protocol Identifier
00  00000000  TP-Data-Coding-Sheme
ff  11111111  TP-Validity-Period

15  00010101  SMS_LENGTH          : 21
              SMS_TEXT            : Hallo jo, das geht ja
```

Tafel 66: Die Meldung CP DATA beim Senden einer Nachricht

12.3 Eine EMS empfangen

Der technische Sachverhalt ist in der Empfehlung ETSI TS 123 040 unter dem Begriff EMS (Extended Message Service) beschrieben. Danach lassen sich bis zu 255 SMS zu einer EMS aneinander reihen. Außerdem existieren Steuerelemente die es gestatten Töne Bilder und Animationen zu übertragen. Die erweiterte Message kann also 255x140 = 35 700 Byte umfassen.
Offenbar waren das Überlegungen wie man in der Vor-GPRS-Ära MultiMediaMessages übertragen kann.
In modernen Mobiles wird diese Methode aber noch angewandt um längere SMS zu transportieren. Es ist immerhin lästig, wenn man einen SMS eingibt, und kurz vor dem geplanten Ende des Textes ist die Eingabe blockiert weil die 160 Zeichen Grenze erreicht ist.
Beim OT 460 z.B. kann man SMS länger als 160 Zeichen eingeben. Ein Mobile das nur einfache SMS empfangen kann erhält dann die Nachricht in einzelne SMS aufgelöst. EMS fähige Mobils erhalten die EMS im Block dargestellt. Wie das funktioniert soll an einem Trace dargestellt werden.

```
_____[ 11 ]___[ 160257 ]___[ DOWN ]___[ NAS ]_____________

19 01 ab 01  00 07 91 94  71 22 72 30  33 00 9f 44  0c 91 94 71
63 32 13 60  00 00 60 11  20 51 30 53  40 a0 05 00  03 69 02 01
14 74 74 98  0e 4a cf 41  61 37 e8 6d  2f cb c3 6c  36 e8 fe 76
93 cb 72 73  9d cd 06 b5  cb f3 79 f8  5c 06 a5 e9  a0 39 fa 5d
67 93 41 e3  b7 7b 9e 9e  d3 41 6f 33  a8 fd 96 97  41 74 74 d8
0d 02 bd dd  65 10 ba ee  26 cb cb 64  50 d8 4d 06  cd d3 78 7a
1e c4 2e d3  e9 65 f9 dc  05 4a 83 ee  69 36 1b 44  97 e7 41 f4
37 68 fc 6e  c3 df f3 32  68 5e 1f a3  41 e1 76 79  3e 0f 9f cb
2e 50 1a 14  6e 83 e6 6f  b9 3c 0f a2  a3 c3


19  0-------  direction from      : originating site
    -001----  TransactionID       : 1
    ----1001  Protocol Discrim.   : SMS messages


01  00000001  MESSAGE TYPE        : CP DATA

: Length of SMS
ab  10101011  lenght              : 171
: Parameter
01  00000001  Parameter           : 1
00  00000000  Parameter           : 0

: SMSC Address
```

```
07  00000111  lenght              : 7

91  1-------  Extension
    -001----  Type of number      : International number
    ----0001  Numbering plan      : ISDN/telephone numberingplan(E.164/E.163)
94..33        number              : 491722270333

: Message Flags
00  00000000  TP-MTI, TP-MMS, TP-SRI, TP-UDIH, TP-RP

: Message Reference Number
9f  10011111  Reference Number    : 159

44  01000100  Parameter           : ems_type

: Destination address

0c  00001100  length              : 12
91  1-------  Extension           : 1
    -001----  Type of number      : international number
    ----0001  Numb. plan id.      : ISDN/telephony numb. pl. (Rec. E.164/E.163)
94..60        number              : 491736233106

: Protocol Identifier
00  00000000  Protocol Identifier
: Data Coding Sheme
00  00000000  Data Coding Sheme
: Parameter
60  01100000  Parameter1
11  00010001  Parameter2
20  00100000  Parameter3
51  01010001  Parameter4
30  00110000  Parameter5
53  01010011  Parameter6
40  01000000  Parameter7

: User Data
a0  10100000  EMS_LENGTH          : 160
05  00000101  HEADER_LENGTH       : 5
              HEADER              : 00 03 69 02 01
              EMS_TEXT            :
                                   that is an overall wonderfull message i
                                   t should consist of more than  one hundr
                                   ed and sixty letters. i will try to comp
                                   ose such a message.i am sorry tha
```

Tafel 67: Erster Teil einer EMS die wenig größer als 160 Zeichen ist.

Der prinzipielle Aufbau der EMS entspricht dem einer SMS. Zu beachten ist der Eintrag dass es sich um eine ems handelt, und dass dem Text ein Header vorangestellt ist, der anzeigt wieviele Textteile folgen.

```
_____[ 3 ]___[ 161849 ]___[ DOWN ]___[ NAS ]_____________

19 01 54 01  00 07 91 94  71 22 72 30  33 00 48 44  0c 91 94 71
63 32 13 60  00 00 60 11  20 51 30 44  40 3c 05 00  03 69 02 02
e8 20 3a ba  2c 2f 83 d2  73 90 fb 0d  1a bf eb 6e  7a 59 0e a2
bf 41 73 f4  fb 0e a2 a3  cb 20 b8 fc  7d 96 97 e7  73 d0 db 0c
4a bb e1 75  ba 0b 04

19  0-------  direction from      : originating site
    -001----  TransactionID       : 1
    ----1001  Protocol Discrim.   : SMS messages


01  00000001  MESSAGE TYPE        : CP DATA

: Length of SMS
54  01010100  lenght              : 84
: Parameter
01  00000001  Parameter           : 1
00  00000000  Parameter           : 0

: SMSC Address
```

```
07  00000111  lenght              : 7

91  1-------  Extension
    -001----  Type of number      : International number
    ----0001  Numbering plan      : ISDN/telephone numberingplan(E.164/E.163)
94..33        number              : 491722270333

: Message Flags
00  00000000  TP-MTI, TP-MMS, TP-SRI, TP-UDIH, TP-RP

: Message Reference Number
48  01001000  Reference Number    : 72

44  01000100  Parameter           : ems_type

: Destination address

0c  00001100  length              : 12
91  1-------  Extension           : 1
    -001----  Type of number      : international number
    ----0001  Numb. plan id.      : ISDN/telephony numb. pl. (Rec. E.164/E.163)
94..60        number              : 491736233106

: Protocol Identifier
00  00000000  Protocol Identifier
: Data Coding Sheme
00  00000000  Data Coding Sheme
: Parameter
60  01100000  Parameter1
11  00010001  Parameter2
20  00100000  Parameter3
51  01010001  Parameter4
30  00110000  Parameter5
44  01000100  Parameter6
40  01000000  Parameter7

: User Data
3c  00111100  EMS_LENGTH          : 60
05  00000101  HEADER_LENGTH       : 5
              HEADER              : 00 03 69 02 02
              EMS_TEXT            : t there is no counter to show the progre
                                    ss
```

Tafel 68: Zweiterr Teil einer EMS die wenig größer als 160 Zeichen ist.

Man erkennt, dass die EMS (hier) in zwei SMS geteilt geteilt ist.

13 Die Steuerung von Mobiles mit AT-Befehlen

Außer über die Luftschnittstelle kann auf ein Mobile auf drei verschiedene Arten zugegriffen werden. Man spricht von Abschlussmöglichkeiten (Termination) und unterscheidet die auf Bild 40 dargestellten Typen

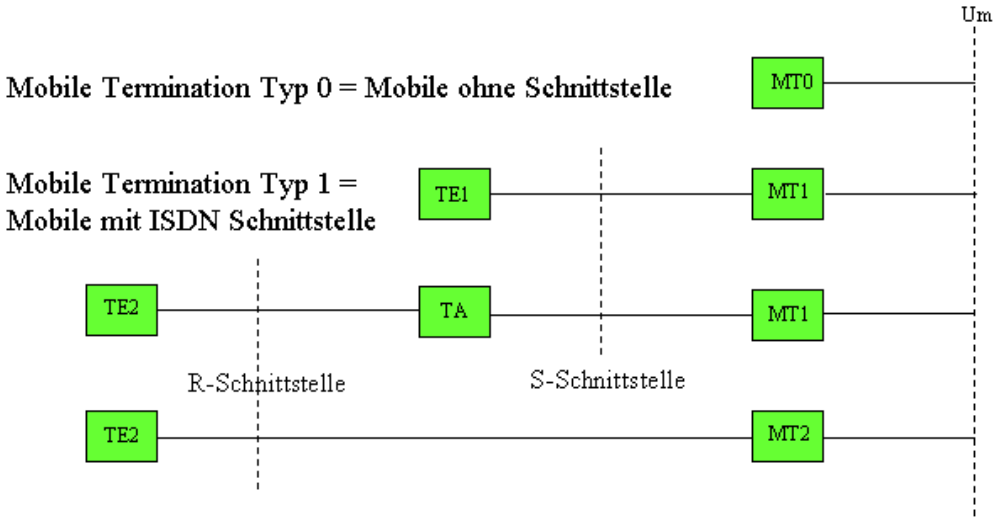


Bild 40: Schnittstellen an der Mobilstation

Mobiles vom Termination Type 1 können über (Soft-) Terminaladapter mit PC-Verbunden werden
Mobiles vom Termination Type 2 besitzen einen eingebauten Terminal Adapter und können direkt an den PC angeschlossen werden.

Das Mobile ohne Schnittstelle wird als Typ 0 bezeichnet. (Es hat lediglich einen Anschluss für das Ladegerät an der Unterseite)
Von einer *Mobile Termination Typ 1* spricht man wenn an das Mobile ein ISDN Endgerät angeschlossen werden kann (Der Typ ist dem Verfasser unbekannt)
Das Motorola TIMEPORT konnte über einen TA angesteuert werden der in Gestalt einer Software (GPRS-WIZARD) auf dem PC installiert werden musste. Es ist daher auch ein MT1.
Unsere Tracemobiles sind vom Typ MT2, sie werden an eine USB-Schnittstelle angeschlossen und wie ein normaler Modem mit AT-Befehlen gesteuert.

Wer seinen Rechner über Modem mit dem Internet verbindet kennt sicher einige AT-Befehle vor allem aus dem Hayes Befehlssatz. Für die Mobilesteuerung werden zusätzliche Befehle benötigt.
In der Empfehlung ETS 300 916 (das ist die GSM 07.07) ist der AT Kommandosatz für GSM-Mobiles niedergelegt.
Dazu gehören sowohl Pflicht-Kommandos als auch optionale Kommandos. Damit kann nicht von vornherein geschlussfolgert werden, welche AT-Kommandos für welchen Mobile-Typ Verwendung finden können. Dazu kommt dass die Hersteller, wie das schon bei den Modems der Fall war, auch noch eigene Kommandos festlegen. Das Thema AT-Kommandos für Mobiles kann hier keinesfalls auch nur annähernd erschöpfend behandeln werden. In drei Abschnitten soll lediglich ein Einblick gegeben werden, wie Dienste, Dienstmerkmale und Kenngrößen eines Mobiles gesteuert werden können.
Das SAGEM OT 460 kann mit Hilfe des HyperTerminal aus dem MS Windows Betriebssystem mit AT-Befehlen gesteuert werden. Dazu koppelt man das HyperTerminal mit dem COM-Port, der im Gerätemanager bei den Anschlüssen (COM und LPT) als Pseudo CDC Modem gefunden wird.

13.1 AT-Kommandos zur Steuerung von Diensten

Bei einem Modem ist üblich, dass die Partnergeräte durch Austausch von *Kenntönen* festlegen, ob die Verbindung der Fax- oder Datenübertragung dienen soll. Außerdem wird durch Austausch von

Der interessiert Leser sollte nun sein Versuchsanordnung wieder aktiviern. Das Herausfinden des COM-Ports über den das jeweilige Mobile mit AT-Befehlen gesteuert werden kann ist je nach Mobiletyp einfach bis unmöglich ☹

Testsignalen die maximal mögliche Bitrate auf der Übertragungsstrecke abgestimmt. Bei Verwendung von Mobiles als Modem wird das Übertragungsverfahrens und die Bitrate wie folgt festgelegt: Mobiles mit den Werten in der nachstehenden Tabelle (Auszug aus GSM 07.07)
Es existiert ein AT Kommando *Select bearer service type.* Es lautet +CBST=[<speed>[,<name>,[<ce>]]]. Will man das Mobile befragen, welchen *Bearer service* es unterstützt Ruft man auf AT+CBST=?

Der Leser kann das mit seinem Mobile sofort ausprobieren. Im Kommandofenster des HyperTerminals wird : AT+CBST=? Eingegeben und die Antworten des Mobiles mit den Werten in der nachstehenden Tabelle (Auszug aus GSM 07.07) verglichen

<speed>:

0	autobauding (Automatischer Auswahl der Geschwindigkeit; diese Einstellung ist möglich bei 3.1 kHz Modem und nicht-transparentem Dienst)
1	300 bps (V.21)
2	1200 bps (V.22)
3	1200/75 bps (V.23)
4	2400 bps (V.22bis)
5	2400 bps (V.26ter)
6	4800 bps (V.32)
7	9600 bps (V.32)
…..	
68	2400 bps (V.110 or X.31 flag stuffing)
70	4800 bps (V.110 or X.31 flag stuffing)
71	9600 bps (V.110 or X.31 flag stuffing)

<name>:

0	data circuit asynchronous (UDI or 3.1 kHz modem)

<ce>:

0	transparent
1	non-transparent

Tabelle 2 : Mögliche Parameter des AT-Kommandos *Select bearer service type* CBST

Wie das beim SAGEM Tracemobile OT 460 aussieht ist in Bild 32 dargestellt.

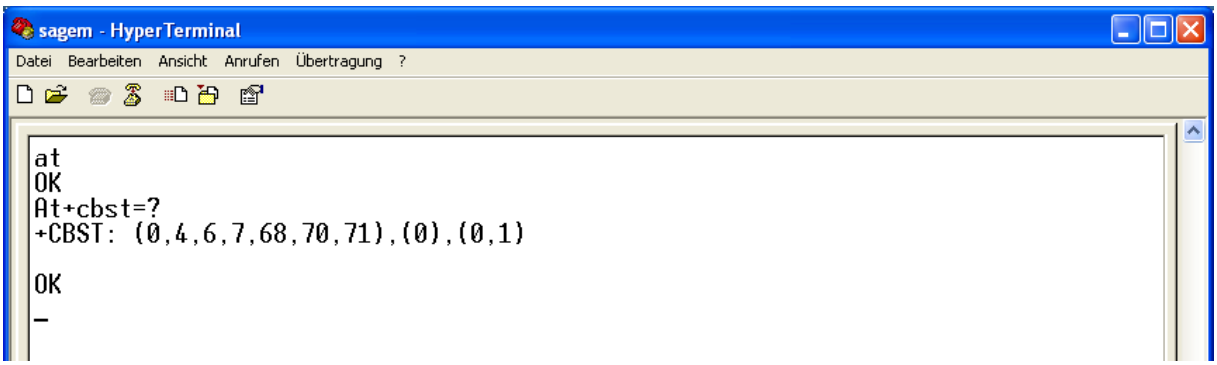


Bild 41: Antwort des OT460 auf AT+cbst=?

Die Liste in Tabelle 2 enthält nur Einträge für Datenübertragung. Da die Übertragung von Sprache eine Hauptfunktion des Mobiles ist, wird der dazugehörende Bearer (speech) einfach durch Anhängen eines Semikolons an die Telefonnummer festgelegt

Ein Anruf von FRITZ!fon entsteht bei Eingabe von
ATD<Nummer von FRITZ!fon>,
in das HyperTerminal

Mit einem OT 460 wurde der Trace an der Luftschnittstelle parallel zum Eingeben des AT-Kommandos mitgeschnitten. Das SETUP entspricht dem auf Tafel 40.

Es soll nun ein Bearer für der Herstellung einer Datenverbindung eingestellt werden. In jedem Falle wird die Übertragungsgeschwindigkeit 9600 bit/sec gewählt und das Übertragungsverfahren Analog-Modem <speed> = 7 , oder Digital-Modem <speed> = 71. In jedem Falle muss <name> = 0, d.h. “data circuit asynchronous (UDI or 3.1 kHz modem)” sein und <ce> = 1, non-transparent.
Damit sieht der AT Kommando String jetzt so aussieht:

AT+CBST =7,0,1 <Enter>
ATD<Ihre Nummer von FRITZ!fon><Enter> für Analogmodem

AT&K3 +CBST =71,0,1 <Enter>
ATD<Ihre Nummer von FRITZ!fon><Enter> für Digitalmodem

In Tafel 69 ist das SETUP auf der Luftschnittstelle dargestellt wenn die AT Befehle für Digitalmodem in das HyperTerminal eingegeben werden.

```
_____[ 9 ]___[ 1019750 ]___[ UP ]___[ NAS ]_____________

03 85 04 07  a1 88 89 21  15 63 a0 5e  07 81 30 73  25 30 17 f5
7c 06 88 90  21 48 40 bb  a1

03  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0011  Protocol Discrim.   : Call control and call related SS messages
85  10------  SendSequenceNumber  : 0

    --000101  MESSAGE TYPE        : SETUP

04  00000100  INFORMATION ELEMENT : Bearer capability
07  00000111  length              : 7
a1  1-------  Extension           : 1
    -01-----  Radio Channel Req.  : full rate support only MS
    ---0----  Coding Standard     : GSM standard coding
    ----0---  Transfer Mode       : Circuit Mode
    -----001  Info Transfer Cap.  : unrestricted digital information
88  1-------  Extension           : 1
    -0------  Compression         : data compression not possible
    --00----  Structure           : service data unit integrity
    ----1---  Duplex Mode         : full duplex
    -----0--  Configuration       : point-to-point
    ------0-  Negot. of Int.      : No meaning is associated with this value.
    -------0  Establishment       : demand
89  1-------  Extension           : 1
    -00-----  Access ID           : octet identifier
    ---01---  Rate Adaptation     : V.110/X.30
    -----001  Signalling Acc.Prot : I.440/450
21  0-------  Extension           : 0
    -01-----  Layer 1 ID
    ---0000-  User Info L1 Prot   : Default layer1 protocol
    -------1  Sync/async          : asynchronous
15  0-------  Extension           : 0
    -0------  Numb Stop Bits      : 1 bit (also used in the case of synchr mode)
    --0-----  Negotiation         : in-band negotiation not possible
    ---1----  Numb Data Bits      : 8 bits (also used i case of bit oriented protocols)
    ----0101  User Rate           : 9.6 kbit/sRecommendation X.1 and V.110
```

```
63  0-------  Extension           : 0
    -11-----  Intermediate Rate   : 16 kbit/s
    ---0----  NIC On Tx           : not require to send data with network  indep.clock
    ----0---  NIC On Rx           : can't accept data with network indep. clock
    -----011  Parity              : none
a0  1-------  Extension           : 1
    -01-----  Connect Element     : non transparent (RLP)
    ---00000  Modem Type          : none

5e  01011110  INFORMATION ELEMENT : CalledPartyBCDNumber
07  00000111  length              : 7
81  1-------  Extension           : 1
    -000----  Type of number      : unknown
    ----0001  Numb. plan id.      : ISDN/teleph. numb. plan (Rec. E.164/E.163) _
30..f5        number              : 03375203717

7c  01111100  INFORMATION ELEMENT : Low Layer Compatibility
06  00000110  length              : 6
88  1-------  Extension           : 1
    -00-----  coding standard     : CCITT standardized coding as described below
    ---01000  inform. transf. cap : unrestricted digital information
90  1-------  Extension           : 1
    -00-----  transfer mode       : circuit mode
    ---10000  transfer rate       : 64 kbit/s -
21  0-------  Extension           : 0
    -01-----  layer1,ident
    ---00001  CCITT standardized rate adaption V.110/X.30. This impl. the presence of octet 5a
              and optionally octet 5b, 5c and 5d as defined below
48  0-------  Extension           : 0
    -1------  synch./ansynch      : asynchronous
    --0-----  negotiation         : in-band negotiation not possible
    ---01000  user rate           : 9.6 kbit/s Recommendations V.6 and X.1
40  0-------  Extension           : 0
    -10-----  intermediate rate   : 16 kbit/s
    ---0----  NIC on Tx           : not required to send data with Network Independent Clock
    ----0---  NIC on Rx           : cannot accept data with Network Independent Clock (i.e.
sender does not support this optional procedure)
    -----0--  Flow control on Tx  : Not required to send data with flow control mechanism
    ------0-  Flow control on Rx  : cannot accept data with flow control mechanism (i.e.
sender does not support this optional procedure)
    -------0  Spare               : 0
bb  1-------  Extension           : 1
    -01-----  number of stop bits : 1 bit
    ---11---  number of data bits : 8 bits
    -----011  Parity              : none

a1  10100001  Information Element : CLIR suppression
```

Tafel 69: SETUP generiert mit Kdo.: AT&K3 +CBST =71,0,1; ATD03375203717

13.2 AT-Kommandos zur Steuerung von Dienstmerkmalen

Als AT Kommando für Dienstmerkmale soll als Beispiel Call Waiting (CW), Ankloppfen dienen . Es lässt sich mit einem AT-Befehl setzen, löschen oder abfragen.

Für eine Übung wird das bereits erprobte handelsübliche Mobile verwendet, das über ein Kabel am PC angeschlossen ist und über den Clienten Hyperterminal gesteuert wird.
Das Mobile wird aus dem ISDN (z.B. von FRITZ!fon aus) angerufen und der Ruf angenommen. Von einem zweiten ISDN-Telefon wird das Mobile ebenfalls angerufen . Man hört (Fabrikeinstellung) den Anklopfton und hat im Soft-Menü die Möglichkeit zu makeln oder den Ruf abzuweisen.
Mit AT-Befehlen besteht nun die Möglichkeit das Verhalten des Mobiles gegenüber Anklopfen zu Steuern.

Der Aufruf erfolgt mit AT+CCWA=[<n>[,<mode>[,<class>]]]

Die Bedeutung der Parameter ist in Tabelle 3 dargestellt .

<n> (sets/shows the result code presentation status in the TA):
0 disable
1 enable

<mode> (wenn der mode Parameter nicht gesetzt ist, wir das Netzwerk nicht befragt):
0 disable
1 enable
2 query status

<class*x*>
1 voice (telephony)
2 data (bezieht sich auf alle Bearer bei <mode>=2)
4 fax (facsimile services)
8 short message service
16 data circuit sync
32 data circuit async
64 dedicated packet access
128 dedicated PAD access

<status>:
0 not active
1 active

Tabelle 3: Mögliche Parameter des AT-Kommandos *Call waiting* CCWA

Man fragt den Status des Dienstmerkmals ab, indem im Hyperterminal das AT-Kommando AT+CCWA=0,2 <ENTER> eingegeben wird. Man erhält die Antwort:

+CCWA: 1,1
+CCWA: 0,2
+CCWA: 0,4

Das bedeutet dass das *Anklopfen* für den Dienste Sprache erlaubt, für Fax und Daten nicht erlaubt ist. *Ankklopfen* für Sprache wird nun ausgeschaltet. Der Befehl lautet AT+CCWA=0,0,1 <ENTER>
Der Befehl zur Abfrage des Status AT+CCWA=0,2 <ENTER> wird nun mit

+CCWA: 0,1
+CCWA: 0,2
+CCWA: 0,4

beantwortet. Rufen man wieder das Mobile mit zwei Telefonen an, muss der zweite Anruf auf *Besetzt s*toßen. Mit dem Kommando AT+CCWA=1,1,1 <ENTER> wird Anklopfen für Sprache wieder erlaubt.

13.3 Allgemeine AT-Kommandos

Zum Schluss sollen noch ein paar GSM-typische AT-Kommandos zur Abfrage interner Werte angegeben werden.

+CGMM Abfrage der Modell Identification
+CGMR Abfrage des Ausgabestandes
+CGSN Abfrage der Seriennummer des Produktes
+CIMI Abfrage der IMSI
+COPS=? Abfrage der zur Verfügung stehenden Operatoren. Das Ergebnis wird als Folge dargestellt (<stat>, Operatorname alphanumerisch in Lang-Form,

Operatorname alphanumerisch in Kurzform, Operatorname in numerischer Form)....(Liste der unterstützten Modi)(Liste der unterstützten Formate).
Es ist <stat>: 0=unbekannt, 1=verfügbar, 2=eingebucht, 3= verboten.

.
.

14. Weiterführende Literatur

14.1 Bücher

[1] Als Standardwerk über GSM kann das Buch:
The GSM System for Mobile Communication, von Michel MOULY und Marie-Bernadette PAUTET , Verlag CELL &SYS, ISBN 2-9507190-0-7
empfohlen werden. Es ist, wie der Titel verrät in englisch geschrieben, aber sehr verständlich detailreich und umfassend. Die Autoren waren an der Entwicklung der Mobilfunk Standards beteiligt. Sehr zu empfehlen!

[2] Sehr detailreich vor allem was die Kommunikation auf der oberen Netzebene zwischen BTS und GMSC betrifft (Base Station Subsystem und Network Switching Subsystem) ist das Buch:
GSM-Signalisierung, verstehen und praktisch anwenden, von Gunnar Heine, Franzis' Verlag 2001, ISBN 3-7723-5774-1
Es ist denjenigen zu empfehlen, die sich tiefer mit der Signalisation auf der Abis und der A-Schnittstelle beschäftigen wollen.

[3] Ein Hochschullehrbuch, das Mobilfunk in voller Breite erklärt, ohne auf Details (Traces der Luftschnittstelle) einzugehen:
GSM Global System for Mobile Communication, von Eberspächer/Vögel/Bettstetter, B.G.Teubner Stuttgart-Leipzig-Wiesbaden,ISBN 3-519-26192-8

[4] Ein Hochschullehrbuch, das Mobilfunk- und Drahtlose Netze in voller Breite behandelt, ohne auf Details (Traces der Luftschnittstelle) einzugehen:
Mobilfunknetze und Ihre Protokolle Band 1, von B. Walke, B.G.Teubner Stuttgart-Leipzig-Wiesbaden,ISBN 3-519-16430-2

[5]Ein Lehrheft in dem die GSM-Dm-Kanäle in Dialogform beschrieben werden, wobei auf der beiliegenden CD u.a. Beispieltrace des ISDN-D-Kanals und der GSM-Dm-Kanäle mit den Tracetools TraceView und GSMView übersetzt werden können:
Die GSM-Dm Kanäle im Dialog, von Joachim Göller,EPV-Verlag Duderstadt, ISBN 987-3-936318-00-5

[6] Die CD enthält einen Experimentalvortrag mit 116 PowerPoint Folien, Übungen auf 26 Power-Point Folien, die Traceübersetzungwerkzeuge EDGEView und ISDNView, sowie einen Lehrtext:
GSMprof-I, CBT-CD von Joachim Göller und Tracemobile SAGEM OT 460, EPV-Verlag Duderstadt,EPV-Best.-Nr.:GPR1

14.2 Technische Spezifikationen

Es werden nur einige grundsätzliche Recommendationen genannt

[1] Die Beschreibung der Meldungen und Informationselemente der Protokolldiscriminatoren 3,5,6,8,10:

ts_100940v070800p GSM 04.08 Digital cellular telecommunications system (Phase 2+); Mobile radio interface layer 3 specification

[2] Die Beschreibung der Schicht 2 Elemente:
ets_300938 . GSM 04.06 Digital cellular telecommunications system (Phase 2+); Mobile Station - Base Station System (MS - BSS) interface; Data Link (DL) layer specification

[3] Die Beschreibung des Formats und der Codierung von Dienstmerkmalen:
ts_124080v030300p Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Mobile radio interface layer 3 supplementary services specification; Formats and coding

[4] Die Beschreibung des Formats von SMS und EMS:
ts_123040v050400p Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Technical realization of Short Message Service (SMS)

[5] Die Beschreibung von AT-Kommandos:
ts_100916v070600p GSM 07.07 Digital cellular telecommunications system (Phase 2+); AT command set for GSM Mobile Equipment (ME)
